



VPOP3 Email Server Manual

© 2017 Paul Smith Computer Services

Note:

To change the product logo for your own print manual or PDF, click "Tools > Manual Designer" and modify the print manual template.

VPOP3 Email Server Manual

© 2017 Paul Smith Computer Services

All rights reserved. This document may be printed for the private use of the downloader. This work may not be edited or modified without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Generated: March 2017

Table of Contents

Foreword	0
Part I Introduction	10
Part II Getting Started With VPOP3	11
1 Preinstallation considerations.....	11
2 Getting to the VPOP3 Settings.....	12
3 Setup Wizard.....	15
Setup Wizard Page 1	16
Setup Wizard Page 2(a)	17
Setup Wizard Page 2(b)	17
Setup Wizard Page 3	18
Setup Wizard Page 4	19
Setup Wizard Page 5	22
Setup Wizard Page 6	22
Setup Wizard Page 7	23
4 Important Setting Checklist.....	24
5 Setting up Email Clients to communicate with VPOP3.....	24
Finding the VPOP3 IP Address	25
emClient	37
Microsoft Outlook 2016	43
Mozilla Thunderbird	52
Part III General Concepts and Terms	58
1 Which programs do what.....	58
2 Editions of VPOP3.....	59
3 Administrators.....	59
4 Email protocols.....	60
POP3	60
SMTP	62
IMAP4	65
SSL/TLS	66
5 Global Address Book.....	67
6 Groups.....	69
7 ISP	70
8 LAN Forwarding.....	70
9 Lists	71
Distribution Lists	72
Mailing Lists	72
10 Mail Connectors.....	73
11 Mappings.....	74
12 Spamfilter Quarantine.....	76

13	Users.....	76
Part IV Procedures		78
1	Add SSL Certificate.....	78
2	Allowing remote users access to their VPOP3 mailboxes.....	79
	Allow Remote Access to VPOP3 without a permanent connection	81
3	Determining your VPOP3 Server Address.....	85
4	Incoming SMTP mail feed.....	89
5	Restoring a backup.....	91
Part V Admin Settings		92
1	Users.....	92
	Adding a User	94
	Editing a User	96
	General	97
	Passwords.....	98
	Routing	100
	WebMail Settings.....	103
	Autoresponder.....	105
	Edit Autoresponder Definition.....	108
	Edit Autoresponder Rule.....	113
	Permissions.....	115
	Aliases	118
	Message Rules.....	119
	Outgoing Sig.....	123
	Internal Sig.....	124
	Advanced.....	125
	Prune Rules.....	128
	Folders	130
	Deleting a User	131
	Manage outgoing message queue	132
	Bulk Actions.....	134
	Import users from file	136
	Import users from Windows	139
	Export users to file	140
	Bulk add users	141
	Edit user welcome message	143
	Send admin message	144
	Bulk edit users	145
2	Lists.....	147
	Using Lists	147
	List Types	148
	Administering Lists	148
	Distribution Lists.....	149
	General	151
	Members	152
	Mailing Lists.....	153
	General	153
	Members	154
	Signature/Headers.....	156
	Subscriptions	158

Other	159
Forwards	161
General	161
Forwarding	162
ODBC Mailing Lists	162
General	163
Signature/Headers	164
Other	165
Groups	167
3 Mappings.....	167
4 Mail Connectors.....	170
Connections	170
Add a Connection.....	171
Edit a Connection.....	172
General	173
Advanced	175
Mail Collectors	176
Add a Mail Collector.....	177
Edit a Mail Collector.....	178
General	179
POP3 General	180
Download Rules.....	183
POP3 Routing	188
Configure Routing Options.....	190
Routing Errors	193
Messages	194
SMTP Options	195
Mail Senders	197
Edit a Mail Sender.....	197
General	198
Settings (SMTP Relay).....	200
Relay Restrictions (SMTP Relay).....	202
Settings (SMTP Direct).....	203
DNS Overrides.....	204
Return Path Settings.....	207
Advanced	209
Domain Filtering.....	210
Connector Schedule	213
5 Services.....	215
General	216
General	216
Global Access Restrictions.....	218
SSL Settings.....	219
POP3	220
General	220
IP Access Restrictions.....	221
Advanced.....	221
SMTP	222
General	223
Filtering	225
SMTP Rules	226
Load Limiting.....	231
IP Access Restrictions.....	232

Spam Reduction.....	234
Edit Realtime Blacklist Rules.....	237
SPF Whitelist	239
VRFY/EXPN.....	240
Advanced.....	241
IDS/IPS	244
IMAP4	247
General	248
IP Access Restrictions.....	249
Advanced.....	249
Password	251
General	251
IP Access Restrictions.....	252
Finger	252
General Tab.....	253
IP Access Restrictions.....	253
LDAP	254
General	254
IP Access Restrictions.....	255
Advanced.....	255
ODBC Database.....	256
WebMail	260
General	261
IP Access Restrictions.....	262
WebMail Settings.....	262
WebAdmin Settings.....	264
Advanced.....	265
Status	266
General	267
Permissions.....	268
IP Access Restrictions.....	269
IP Access Restrictions	269
GeoIP Lookup.....	271
Service Bindings	273
Bandwidth Throttling	274
6 Settings.....	278
Admin Settings	278
General Tab.....	279
Message Targets.....	281
Message Control Tab.....	282
Anti-virus	284
Antivirus General Tab.....	285
Antivirus Incoming Messages Tab.....	286
Antivirus Outgoing Messages Tab.....	288
Antivirus Updates Tab.....	289
Attachment Processing	289
Filtering	290
Attachment Processing Advanced Filter Rules.....	293
Filtering Conditions.....	299
Extraction.....	301
Autoresponder Settings	302
Database	304
Backups	305
Query	307

Connection.....	309
Message Store.....	311
Amazon S3 Backup.....	314
Restore	320
Offsite Backup.....	323
Diagnostics	324
General	325
Session Logs.....	327
Temporary/Archived Files.....	329
Log File Sizes	330
Retention.....	331
Message Trace.....	333
Message Search.....	334
Log File Writer.....	336
SysLog	337
Global Signature	339
Groups	342
Header Processing	344
Receipts/Urgent Messages.....	344
Urgent Messages.....	344
Receipts	345
Global Header Modifiers.....	346
Legacy Extensions	347
Local Mail	348
General	349
Domain Mappings.....	350
LAN Forwarding.....	351
Configuration	352
Configure LAN Forwarding Server Address Verification for Wildcards	355
Queue Status	357
Logging	358
Message Archiving	360
General	361
Extra Archive Actions.....	362
Search	367
Results	368
Offline	369
Maintenance.....	371
Technical Information.....	371
Message Authentication	372
Authentication Results.....	372
BATV	373
Message Monitoring	375
Misc Settings	376
General	377
Permissions.....	379
Disk/Memory Checking.....	380
External Fax.....	381
Proxy	382
Advanced.....	383
Bandwidth Pools.....	388
Quotas	389
Scripts	391

Security Settings	392
General	392
Intrusion Protection.....	394
Spam Filter	395
General	395
General	396
Quarantine Settings.....	397
Bayesian Database.....	399
Script Configuration.....	401
Rule Weights	404
Advanced	406
White/Black Lists.....	407
Whitelist Addresses.....	408
Blacklist Addresses.....	410
Whitelist Words.....	412
Blacklist Words.....	413
Quarantine Viewer.....	414
VPOP3 Text Strings	417
7 Status	418
Dashboard	418
Server Status	419
Sessions	420
8 Reports	421
Messages Received	422
Messages Sent	423
Message Summary	424
Largest Folders	425
Quotas	426
SMTP Server Status	428
SMTP Usage	429
Spam Filter	431
9 About	433
Part VI Reference	436
1 CIDR	436
2 Creating a Dial-Up connection for VPOP3 to use	439
3 Email File Types	443
4 File path macros	444
5 Lua Scripting	444
IDS Log Formatter Script	445
Signature Script	445
SMTP Rule Scripts	447
6 PostgreSQL installation details	449
vpop3postgres user account	450
7 Regular Expressions	450
8 SMTP MX Sending	451
9 Spamfilter	452
Quarantine	453
Bayesian Filter	454

10	Summary Log File Format.....	455
11	VPOP3 Service Controller.....	456
12	VPOP3 Status Monitor.....	458
13	VPOP3.INI format.....	463
14	Wildcards.....	465
Part VII Trouble Shooting		466
1	BCC Messages and catch-all POP3 mailboxes.....	466
2	Event Log Problems.....	467
3	Troubleshooting login problems.....	469
	Index	470

1 Introduction

Thank you for using our manual for the VPOP3 Mail Server

This manual is currently a 'work in progress' which may mean that you find missing topics, or topics not containing text. Please bear with us while we are working on this.

You may find more up-to-date information in our [Wiki](#). If a topic is missing from both this manual and our Wiki, then, as long as you are using the [current version of VPOP3](#), feel free to email support@pscs.co.uk with a request for the topic to be added, and we will treat that request more urgently than the normal manual updates.

Please note that we have several sections on our website which contain information which may be useful to you:

Our Wiki

Our [Wiki](#) contains lots of useful information, including reference information, 'How To's, troubleshooting tips, details on error messages, etc

Forum

Our [Forum](#) is a place for asking questions or searching previous questions & answers about VPOP3. This section can be used even if you do not have an active support or maintenance contract, but the response is not guaranteed, and the sections for older versions of VPOP3 are not actively monitored by our technical support staff

BugTracker

Our [bug tracker](#) contains details on issues which have been reported to us, current state, workarounds etc. It also contains feature requests and so on. Users can sign up to receive tracking information on issues/features, or even report issues themselves.

The bug tracker also has '[roadmap](#)' and '[changelog](#)' sections so you can see what we have planned for upcoming releases, and what changes have been made in existing releases.

Blog

Our [Blog](#) is where we post articles on VPOP3 (and other topics). This includes new releases, and detailed information on new features which we think you may find interesting.

2 Getting Started With VPOP3

2.1 Preinstallation considerations

Requirements

- Windows XP **or later**. That means it will work on Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 2003, Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2, Windows SBS 2003, Windows SBS 2008, Windows SBS 2011, Windows 2016, Windows 2017, Windows 2018, Windows 2019 etc, etc, etc **or any later version**. If Microsoft bring out a new version of Windows and it's not in this list, VPOP3 will work on it unless we say otherwise because it will work on Windows XP **or later**. There are 32 and 64 bit (starting from v7.1) versions of VPOP3. The 32 bit version will work on either 32 or 64 bit versions of Windows. The 64 bit version requires a 64 bit version of Windows
- 1GB RAM - it may work on less, but it may be slow. It will work better with more RAM
- 1GHz processor. VPOP3 can use multiple cores/processors if available.
- 100MB Disk space - it can be installed with 100MB disk space, but it will undoubtedly need more for data storage. How much will depend on many factors, such as how many [users](#) you have, how much mail will be stored on the server, whether you will be [Archiving](#) email etc. Also, by default VPOP3 will make daily backups of its own database, so you should have space to store these if possible.
- Internet connection (broadband or dialup)
- Web browser (Google Chrome & Mozilla Firefox are recommended, but it should work with Opera, Apple Safari and Microsoft Internet Explorer 8 or later)

Recommendations

- If you have large numbers of users using [IMAP4](#) with [VPOP3 Enterprise](#) then you will probably find that the disk I/O will be the limiting factor before the CPU. This can be helped by having more free RAM available for disk caching, and having a faster disk I/O subsystem - e.g. SAS drives instead of SATA drives, RAID 10 arrays, hardware RAID controller with battery backed/non-volatile write cache, etc.

Things to watch out for

- We do not recommend using RAID 5 arrays. VPOP3 uses a database server (PostgreSQL), and RAID 5 arrays often encounter performance issues with databases, because of frequent small writes to the disk. With a RAID 5 array a write requires a read from all disks and then a write back to all disks. Generally, it is not recommended to use a RAID 5 array with databases which perform many writes to disk (as the VPOP3 database does).
- Take care if you are using 5400 RPM SATA drives. You will probably find that these are too slow to handle many users, because of the very slow access times.
- You should turn off any write-back caching on the disks on the VPOP3 PC. If you don't do so, then power failures (or hard shutdowns) may cause database corruption, requiring you to restore the database from a backup. The exception is if you have a hardware RAID controller with battery backed write cache (BBWC) or non-volatile write cache (NVWC). In this case, the hardware will remember any data waiting to be written back to the disk in the case of power failure, and will write it to the disks once the power is restored.

- Virus scanners can cause problems. If you install a third party virus scanner on the VPOP3 PC, we recommend that you exclude the *VPOP3\pgsql\data* folder (and sub-folders) from any virus scanning, and turn off any email scanning on that PC. If you want to scan emails as they are received by and sent by VPOP3, then either use one of our integrated virus scanners, or use a specialist email server virus scanner, rather than a normal desktop virus scanner.
- Backup software should not backup the *VPOP3\pgsql\data* folder unless it uses VSS (Volume Snapshot Service). If the files in that folder are accessed by other software, the database server used by VPOP3 may be unable to access the files when it needs to, causing database issues.

2.2 Getting to the VPOP3 Settings

You access the VPOP3 settings through a web browser.

Server Address

By default, to access the settings, you will go to:

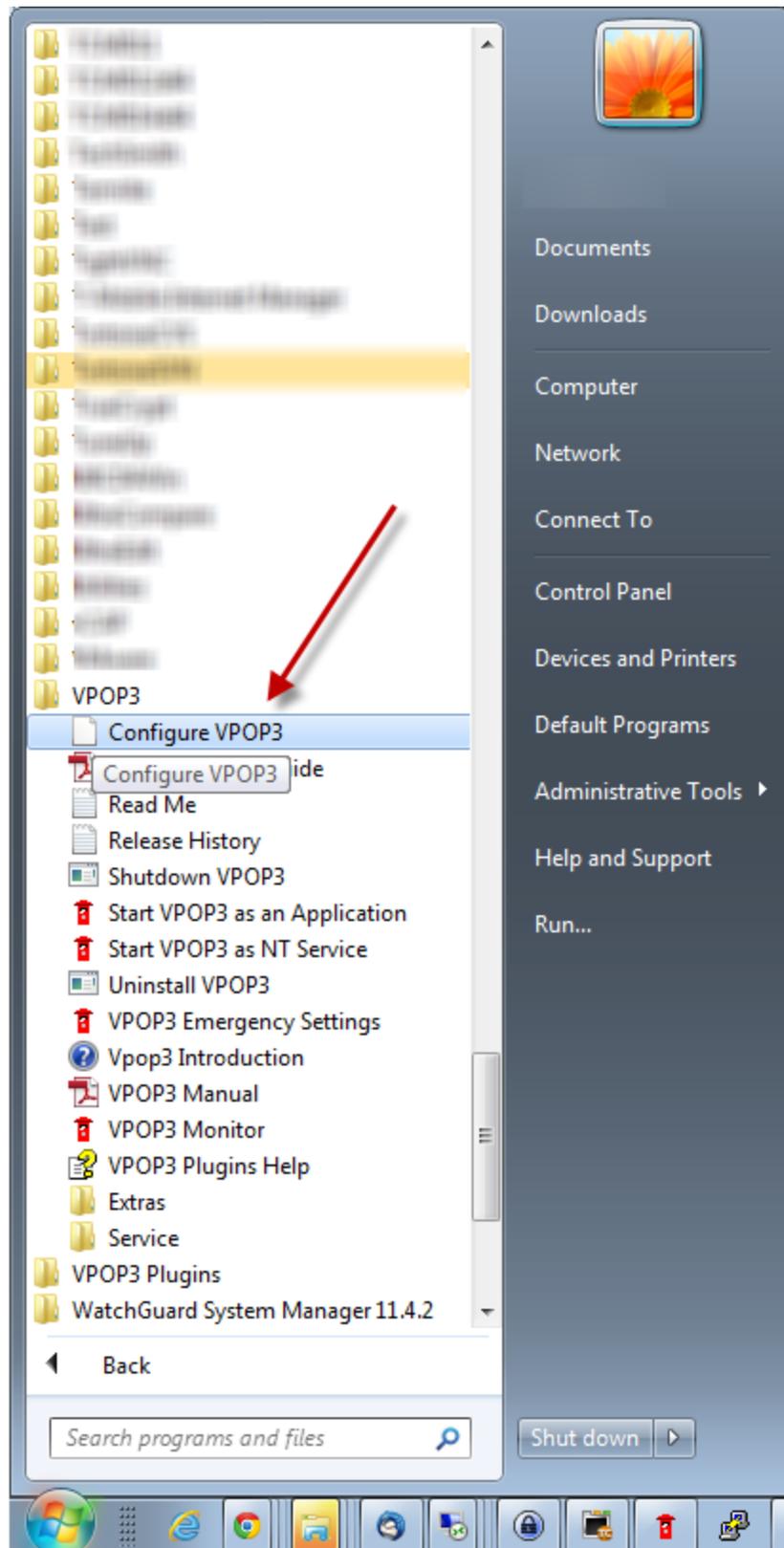
`http://<server IP address>:5108/admin/index.html`

On the VPOP3 computer itself, you can use:

<http://127.0.0.1:5108/admin/index.html>

Shortcut from the Start Menu

On the VPOP3 computer itself, go to **Start » All Programs » VPOP3 » Configure VPOP3**

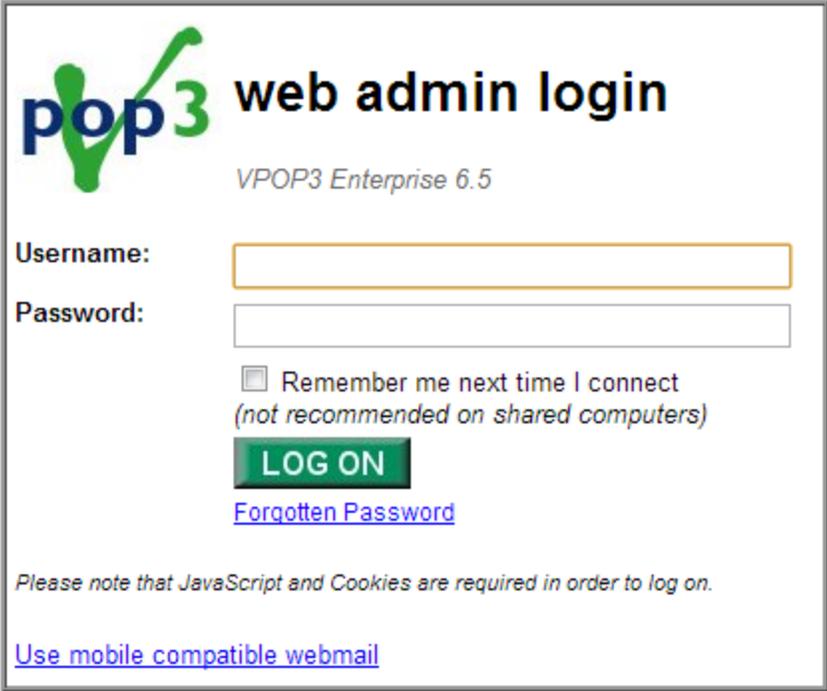


Shortcut from the Status Monitor

If you have the VPOP3 status monitor on your PC, then you can right-click the icon () and choose **VPOP3 Settings** from the pop-up menu.

Logging in

Once you are seeing the login page, then you need to log in with the administrator login details.



pop3 web admin login
VPOP3 Enterprise 6.5

Username:

Password:

Remember me next time I connect
(not recommended on shared computers)

LOG ON

[Forgotten Password](#)

Please note that JavaScript and Cookies are required in order to log on.

[Use mobile compatible webmail](#)

Login page

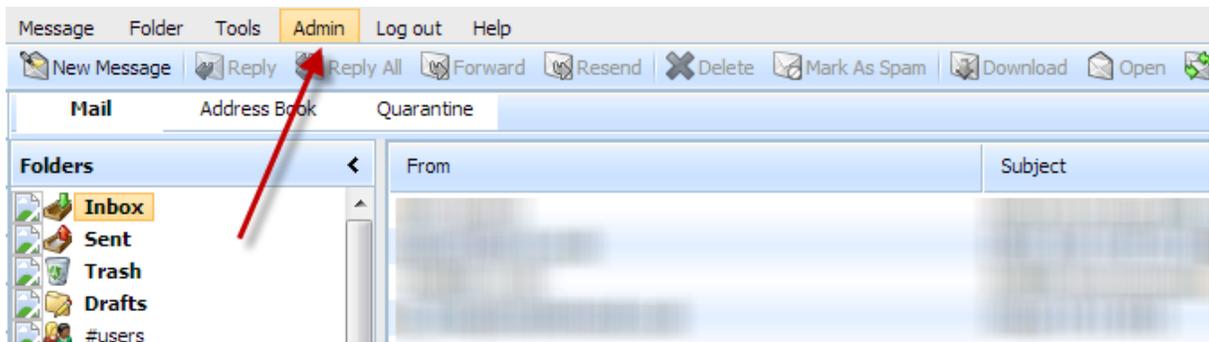
The username & password to use when logging in are those used for an [administrator](#) user.

The default login details are:

➤ Username: *postmaster*

➤ Password: *admin*

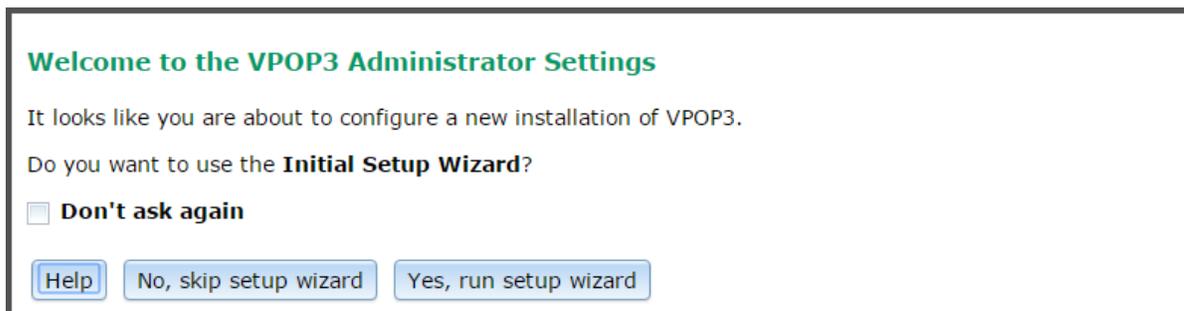
If, after logging in, you find yourself in the Webmail instead of the Admin settings, then there should be an **Admin** item on the Webmail menu. Clicking that will take you to the VPOP3 Settings.



If the **Admin** link isn't there, then there are two possibilities:

- the login details you are using are not for an administrator
- VPOP3's [Access Restrictions](#) are denying administration access from your IP address. In this case, try accessing the VPOP3 settings using <http://127.0.0.1:5108/admin/index.html> from the VPOP3 computer itself or see [this article](#) in our Wiki.

2.3 Setup Wizard



When you run VPOP3 without it having been configured, then you will be given the option of running the Setup Wizard. The Setup Wizard will configure VPOP3 for a very simple, but typical, configuration, with a single ISP mail account. Everything you configure in the Setup Wizard can be modified easily later, so it is usually a good idea to run the Setup Wizard as it will configure things that you may otherwise miss.

You have the option of Skipping the wizard or running it. If you skip the wizard you can check the **Don't ask again** box so you won't be prompted to run the wizard the next time you log in.

If you have skipped the wizard and want to run it at a later stage, in your web browser's address bar, go to **http://<server IP address>:5108/admin/index.html?firstconfig=1**. Note that you *should not* do this if you have already configured VPOP3 as it may overwrite some of your settings.

➤ [Start the Setup Wizard](#)

2.3.1 Setup Wizard Page 1

Setup Wizard (Page 1 of 7)

This Wizard takes you through the initial basic setup process for VPOP3.

Please note that this only takes you through the most basic settings for VPOP3. There are many more options available from within the main settings pages. You can create multiple connection methods, email sending and collection methods, and schedules as well as user aliases, lists, etc all from within the main settings pages.

How do you want VPOP3 to connect to the Internet?

LAN Connection (eg router, proxy server or firewall)

Dial-up Connection (RAS, modem)

Import settings from

Use settings for ISP

Manual setup

Please note - imported settings are not guaranteed to be correct, please check them yourself.

The ISPs listed on this page are not *recommended* ISPs, they are simply the ISPs whose details we know. They are typically no better or worse than other ISPs who may not be listed. If you know the details of an ISP which is not listed, email the details to support@pssc.co.uk and we will be pleased to add it to the next release of VPOP3.

First, you can choose how VPOP3 will connect to the Internet. Usually you will choose **LAN Connection** if VPOP3 is connecting through a router or firewall. Only choose **Dial-up Connection** if VPOP3 is to be responsible for dialing a modem itself.

Then, you can choose to

1. **import settings from** an email client installed on the VPOP3 PC, in the same user account which VPOP3 is using. This is rarely useful.
2. use settings we have been told about a specific ISP. This will configure mail servers etc for that ISP. Note that this information has been provided to us by third parties so may not be correct or up to date, so you should check the details.
3. manually configure the mail server settings required by your ISP. This is usually the best option. Your ISP will be able to tell you the incoming and mail server names that you need to use, and your username & password.

Whichever of these options you choose, the next page will depend on whether you are connecting using LAN or dial-up. If you import the settings from somewhere, it will simply pre-populate the setting fields you will see on the later pages.

- [Use LAN Connection](#)
- [Use Dial-up Connection](#)

2.3.2 Setup Wizard Page 2(a)

Setup Wizard (Page 2 of 7)

You have specified that VPOP3 will connect over a LAN connection. In this case VPOP3 doesn't need to know any more about the connection. Make sure that the Windows networking **Default Gateway** and **DNS Servers** are set correctly. These may be set automatically by your router, or may need manual configuration in the Windows networking settings.

If you want to change this setting in the future use the **Mail Connectors -> Connections** Page

What is the name of your ISP?

Help << Back Next >> Cancel

On this page you just need to enter the name of your ISP. This does not change VPOP3's behaviour, but is simply for your reference and will appear in the setting screens and error messages.

> [Next page](#)

2.3.3 Setup Wizard Page 2(b)

Setup Wizard (Page 2 of 7)

When adding a Connection method which connects using a dial-up connection, VPOP3 needs to know the details of the dial-up connection to use. These are usually obtained from your Internet provider (the company that supplies you with internet connectivity).

The dial-up connection should first be configured within Windows and tested to ensure that it works correctly. Make sure it is available to ALL USERS.

If you want to change this setting in the future use the **Mail Connectors -> Connections** Page

Dial-up Connection VPOP3 should use :

Dial-up Username :

Dial-up Password :

Help << Back Next >> Cancel

Choose the dial-up connection which VPOP3 should use here, and enter the username & password to connect to your ISP using that connection.

Note that, because VPOP3 is running as a service, it can only see dial-up accounts which have been configured to be usable by anyone on the VPOP3 PC (not "shared", because that uses the Internet Connection Sharing service, which is different). See the [Creating a Dial-Up connection for VPOP3 topic](#) for more information.

> [Next page](#)

2.3.4 Setup Wizard Page 3

Setup Wizard (Page 3 of 7)

Configure the method VPOP3 uses for sending outgoing mail

If you want to change this setting in the future use the **Mail Connectors -> Senders** Page

How do you want VPOP3 to send outgoing mail :

- via your ISP's SMTP relay server** (or 'SmartHost'). Choose this option if your ISP have told you a mail server for sending outgoing mail
- Directly to the recipient's mail server.** Choose this option if your ISP do not have a relay server you can use. We do not recommend this option if you use a dial-up connection, or if you have a dynamic IP address assigned by your ISP.

SMTP Relay Settings

SMTP Relay Servers:

SMTP Authentication

This server requires SMTP authentication

SMTP Username:

SMTP Password:

This page lets you configure VPOP3 for sending outgoing mail.

For most small businesses you will want to choose the **via your ISP's SMTP relay server** option. Use this option if your ISP has provided you with an SMTP relay server (or 'smarthost') to send your outgoing mail through. This is the same as how you would send mail from a normal email client such as Mozilla Thunderbird or Microsoft Outlook.

Bigger companies who have leased lines or co-located servers may wish to send **directly to the recipient's mail server**. With this option, VPOP3 looks up MX DNS records and sends messages directly to the recipient's mail server. This is quite different from how a normal email client would work. It is more complex to get working reliably because many big mail providers set special conditions for which servers they will accept mail from (e.g. reverse DNS, IP addresses not being in certain 'dial-up lists' and so on). Also, you will see VPOP3 being unable to send messages and retrying, which can confuse some people. With the first option, this retrying is carried out invisibly by your ISP's smarthost so you can't see it; with the second option, VPOP3 is managing the retrying, so you can see it.

If you use the **via your ISP's SMTP relay server** option, then you should enter the relay server address, and username/password, if required, in the boxes on this page.

If you use **directly to the recipient's mail server**, then the lower half of the page changes as below:

SMTP Direct Settings

SMTP Direct sending tells VPOP3 to ask a DNS server for the MX records for the recipient's email domain. VPOP3 then tries to send the messages directly to the designated mail servers for that domain. If the recipient's mail server does not respond, VPOP3 will try to send the message again later.

DNS Servers to use :
(separate multiple DNS servers with commas, leave blank to autodetect)

In this case, just enter the DNS servers to be used by VPOP3 (or leave blank to use the DNS servers used by Windows). VPOP3 needs a reliable DNS server to perform direct sending, as it uses DNS to discover which mail server should be used for each recipient email domain.

Note - if you don't want VPOP3 to send outgoing mail at all, choose **via your ISP's SMTP relay server**, and leave the **SMTP Relay Servers** box empty.

> [Next page](#)

2.3.5 Setup Wizard Page 4

Setup Wizard (Page 4 of 7)

Configure the initial Collector which VPOP3 uses for collecting incoming mail.

If you want to change this setting, or add more Collectors in the future go to **Mail Connectors -> Collectors**.

How do you want VPOP3 to collect incoming mail: ▼

Incoming POP3 Settings

This option makes VPOP3 retrieve messages from a POP3 mail server at your ISP.

POP3 Server Address :

POP3 Authentication Method : ▼

POP3 Account Username :

POP3 Account Password :

Routing Method : ▼

Target User : ▼

This page lets you set up how VPOP3 gets incoming mail.

In **How do you want VPOP3 to collect incoming mail** there are three options:

- **From an ISP's POP3 email account** - this is the normal situation with email for individuals or small businesses. Your ISP will have provided you with a POP3 mail server address and username & password details.
- **Through an incoming SMTP feed** - you can use this option if you have a fixed IP address and can set the MX DNS records for your domain to point to that IP address (see [this knowledgebase article](#) for more details)
- **Using ODMR (On Demand Mail Relay/ATRN)** - this option is provided by some ISPs for business accounts. You will know if you have to use this because your ISP will have told you.

From an ISP's POP3 email account

Use this option if your ISP has given you POP3 email account details. Note that the setup wizard only allows you to set up collection from a single POP3 account, but VPOP3 can download from many different accounts, you can set these up later in the **Mail Connectors** -> [Mail Collectors](#) section of VPOP3.

Enter the POP3 email account details provided to you by your ISP into the **POP3 Server Address**, **POP3 Account Username** and **POP3 Account Password** boxes. The **POP3 Authentication Method** option will usually be **Plain Text**, but **APOP** or **CRAM-MD5** will be more secure if your ISP supports those options. You can change this information later by editing the Mail Collector in **Mail Connectors** -> **Mail Collectors**.

For the **Routing Method**, you can choose:

- **Parse Message Headers** - use this if the POP3 mailbox contains mail for multiple people - eg it is a catch-all mailbox
- **All messages to a single user** - use this if the POP3 mailbox contains mail for just a single user or email address
- **All messages to a single user on another server** - use this if the POP3 mailbox contains mail for just a single user and you want VPOP3 to send that mail to a different local mail server

Parse Message Headers

The **Accepted Domains** setting tells VPOP3 which email domains or addresses to expect in this POP3 account. Separate multiple entries with ';' (semicolon) characters.

Accepted Domains :

If you choose this option, VPOP3 will look at the To, and Cc message headers to see who the message is for. You have to tell VPOP3 which email domains it will accept mail for. This is so that it can ignore email addresses in the To or Cc headers which don't apply to you. Enter the domains in the **Accepted Domains** box, separated by semicolons if you have more than one domain's email coming into this POP3 account

All messages to a single user

Routing Method :

Target User :

If you choose this option, VPOP3 will send all mail downloaded from this POP3 account to a single user's mailbox. This is used when the POP3 account on the ISP only contains one user's messages.

Choose the mailbox for the messages to go to in the **Target User** box. (Note that if you are just setting up VPOP3 from scratch, you may only be able to select the default user here. You can change this later in **Mail Connectors -> Mail Collectors**.)

All messages to a single user on another server

Routing Method : All messages to a single user on another server ▾
This option forwards to a single email address on the other mail server. To forward to several different email addresses on the other mail server choose the 'Parse message headers' option here and use the Main LAN forwarding configuration on Settings -> LAN Forwarding
Target email address : <input type="text"/>
Target email server : <input type="text"/>

If you choose this option, VPOP3 will send all mail to a single email address on another local server. Use this if the ISP POP3 account only contains one user's messages and you have a separate server, such as Microsoft Exchange where you want messages to be sent to.

If the ISP POP3 account contains mail for multiple users, then choose **Parse Message Headers** and set up LAN Forwarding in [Settings -> Local Mail -> LAN Forwarding](#).

Through an incoming SMTP feed

Incoming SMTP Settings
This option means that VPOP3 will receive email by messages being sent directly to VPOP3's SMTP service by a remote mail server. VPOP3 will actually always accept messages sent to it using SMTP. These settings are only needed if VPOP3 has to do something (such as dial a connection, or send an ETRN command to a remote server) in order to trigger the remote server to start sending the messages.
Email domains to accept : <input type="text" value="*@company.com"/>
Wait for up to : <input type="text" value="60"/> seconds for an incoming SMTP connection
<input type="checkbox"/> Use ETRN
Server to send ETRN to : <input type="text"/>
Parameters for ETRN : <input type="text"/>

If you choose this option, then VPOP3 will accept incoming mail using SMTP. Note that VPOP3 will accept incoming SMTP mail in any case (as long as your firewall is configured to allow incoming SMTP connections), but using this option will tell VPOP3 to wait for incoming connections if using a dial-up connection, or trigger a remote server to start sending you queued messages by using the ETRN command.

If you want to have direct incoming SMTP without going through an ISP's server, then enter your email domains in the **Email domains to accept** box, and select **Wait for up to "1" seconds**

➤ [Next page](#)

2.3.6 Setup Wizard Page 5

Setup Wizard (Page 5 of 7)

Configure what email VPOP3 treats as local mail

If you want to change this setting in the future use the **Settings -> Local Mail** Page

Specify the email domain(s) which are to be handled locally (usually this is your normal email domain).

Local Domains :
(separate multiple domains with semicolons)

This domain setting is also used to determine which incoming SMTP or ODMR mail should be accepted.

This page lets you set which email addresses are treated as local. Mail to local email addresses will not go out to the Internet at all (unless using [*REMOTE mappings](#)). This setting is also used for incoming SMTP or ODMR mail feeds.

Enter your local domain(s) in the **Local Domains** box. If you have multiple domains, separate them with semicolons (;)

➤ [Next page](#)

2.3.7 Setup Wizard Page 6

Setup Wizard (Page 6 of 7)

Configure how often VPOP3 collects and sends email

This page lists several common options for the connection schedule. Please choose the most appropriate one for your situation. Note that connection schedules are highly customisable from the **Mail Connectors -> Schedule** page later.

At what times do you want VPOP3 to automatically collect/send email :

Never
 During working hours
 24 hours a day

On what days do you want VPOP3 to collect/send email :

Weekdays only
 Weekends only
 All days

How often do you want VPOP3 to collect/send email :

Every 10 minutes
 Every hour
 Every 2 hours

This page lets you tell VPOP3 how often to check for mail from external POP3/ODMR accounts, how often to send mail out, and how often to check for spamfilter or antivirus updates if you are using those options.

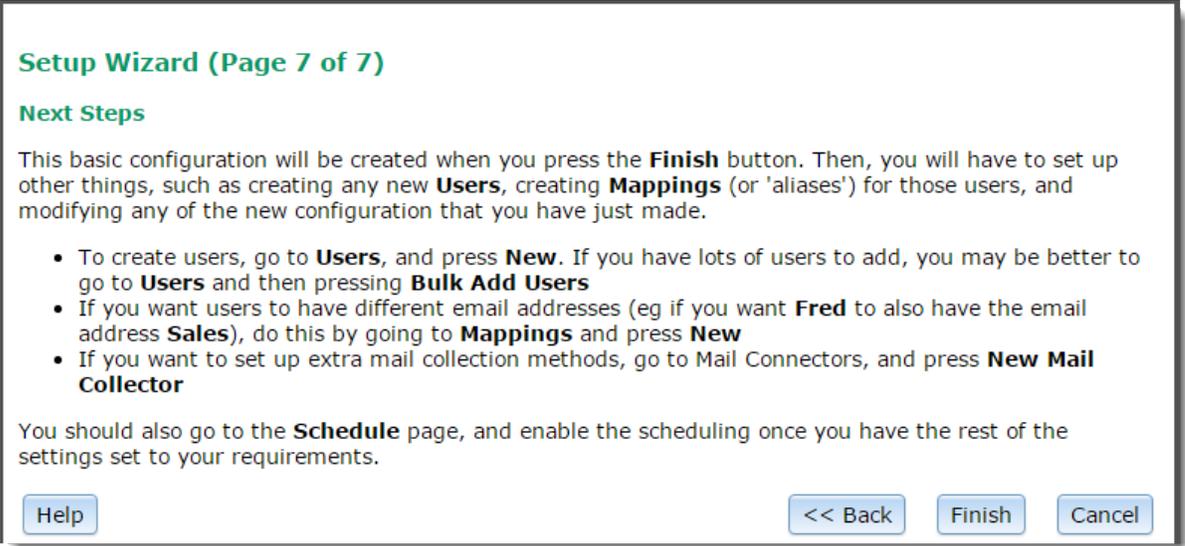
You can choose a standard 'template' of how often, and when VPOP3 should 'poll' for messages.

If you have a permanently-on Internet connection then you should probably choose **24 hours a day - All days - Every 10 minutes**.

Note that you can change these settings later, with more options, in the [Mail Connectors -> Connector Schedule](#) page later.

➤ [Next page](#)

2.3.8 Setup Wizard Page 7



Setup Wizard (Page 7 of 7)

Next Steps

This basic configuration will be created when you press the **Finish** button. Then, you will have to set up other things, such as creating any new **Users**, creating **Mappings** (or 'aliases') for those users, and modifying any of the new configuration that you have just made.

- To create users, go to **Users**, and press **New**. If you have lots of users to add, you may be better to go to **Users** and then pressing **Bulk Add Users**
- If you want users to have different email addresses (eg if you want **Fred** to also have the email address **Sales**), do this by going to **Mappings** and press **New**
- If you want to set up extra mail collection methods, go to Mail Connectors, and press **New Mail Collector**

You should also go to the **Schedule** page, and enable the scheduling once you have the rest of the settings set to your requirements.

[Help](#) [<< Back](#) [Finish](#) [Cancel](#)

The final page of the Setup Wizard does not contain any settings, but gives a list of things you may want to do later, and where in the VPOP3 settings you should go to configure them. The details are copied below for your reference.

Next Steps

You will have to set up other things, such as creating any new [Users](#), creating [Mappings](#) (or 'aliases') for those users, and modifying any of the new configuration that you have just made.

- To create users, go to [Users](#), and press [New](#). If you have lots of users to add, you may be better to go to [Users](#) and then pressing [Bulk Add Users](#)
- If you want users to have different email addresses (eg if you want Fred to also have the email address Sales), do this by going to [Mappings](#) and press [New](#)

- If you want to set up extra mail collection methods, go to [Mail Connectors](#), and press [New Mail Collector](#)

You should also go to the [Schedule](#) page, and **enable the scheduling** once you have the rest of the settings set to your requirements.

2.4 Important Setting Checklist

This is a list of the settings you should make sure are set in VPOP3 for 'normal' configuration:

- ❖ [Local Domains & Default Domain](#)
- ❖ A [Connection](#) is created
- ❖ [Mail Collector\(s\)](#) are created if necessary
- ❖ A [Mail Sender](#) is created if necessary
- ❖ A [Connection Schedule](#) is created
- ❖ [Users](#) & [Mappings](#) (if necessary) are created

2.5 Setting up Email Clients to communicate with VPOP3

Setting up email clients to communicate with VPOP3 is straightforward. VPOP3 is a POP3/SMTP (and IMAP4 if you have [VPOP3 Enterprise](#)) email server, just like an ISP's mail server, so you set up the email client just as you would for any other email service, but using the VPOP3 server address as the incoming & outgoing mail server, and using the username & password defined in VPOP3 as the login details.

There are very many email clients available, so we can't give step-by-step instructions for all of them, but some are given below. For other email clients just use the basic concept above. The email client documentation should be able to help with the specifics of where you enter the relevant details.

When setting up the email client, you need to know the IP address of the VPOP3 server. See the [Finding the VPOP3 IP Address](#) topic for how to do that.

Email Clients

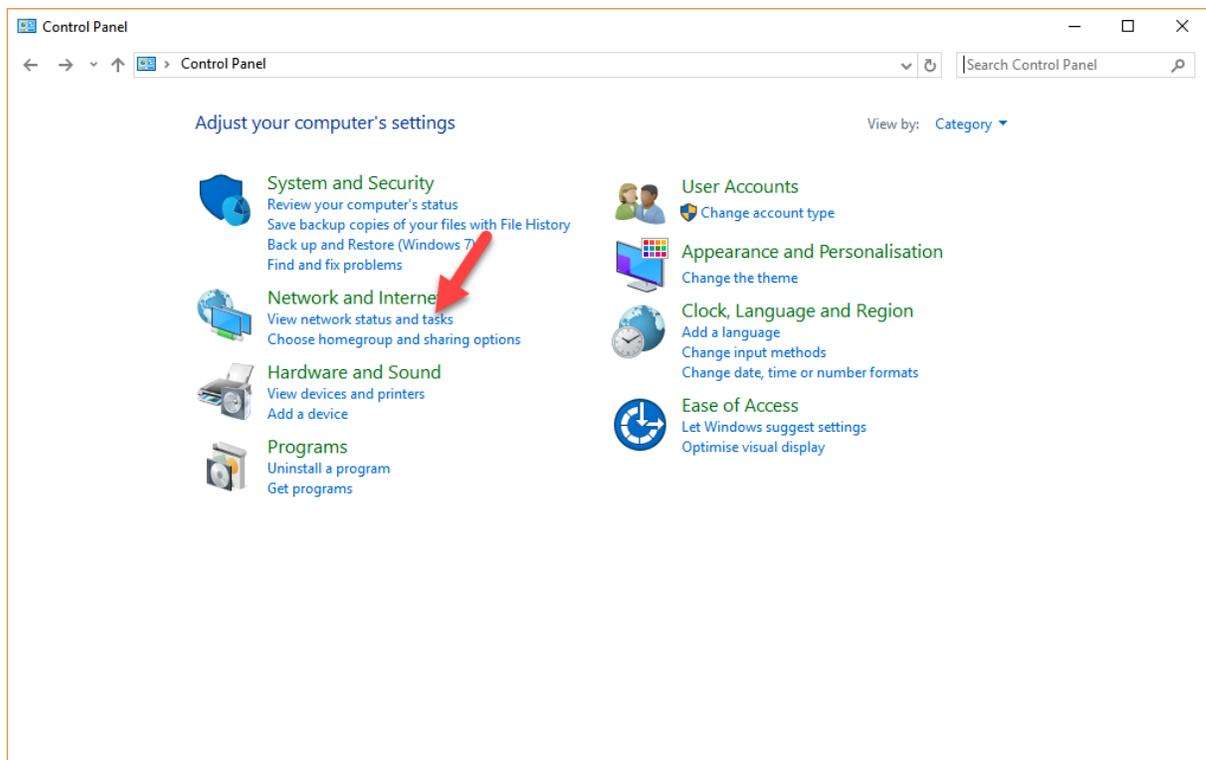
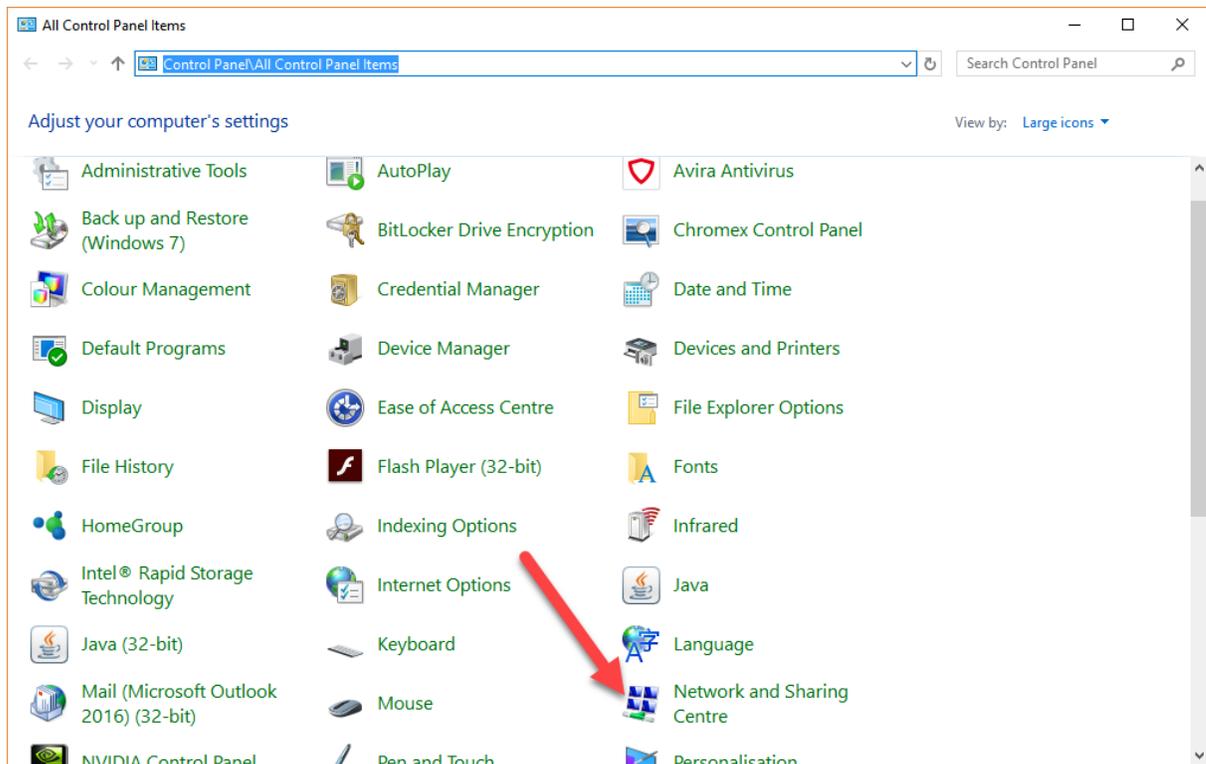
- [emClient](#)
- iPod/iPhone email client
- Mac Mail
- [Microsoft Outlook 2016](#)
- [Mozilla Thunderbird](#)
- The Bat!
- Windows Live Mail

2.5.1 Finding the VPOP3 IP Address

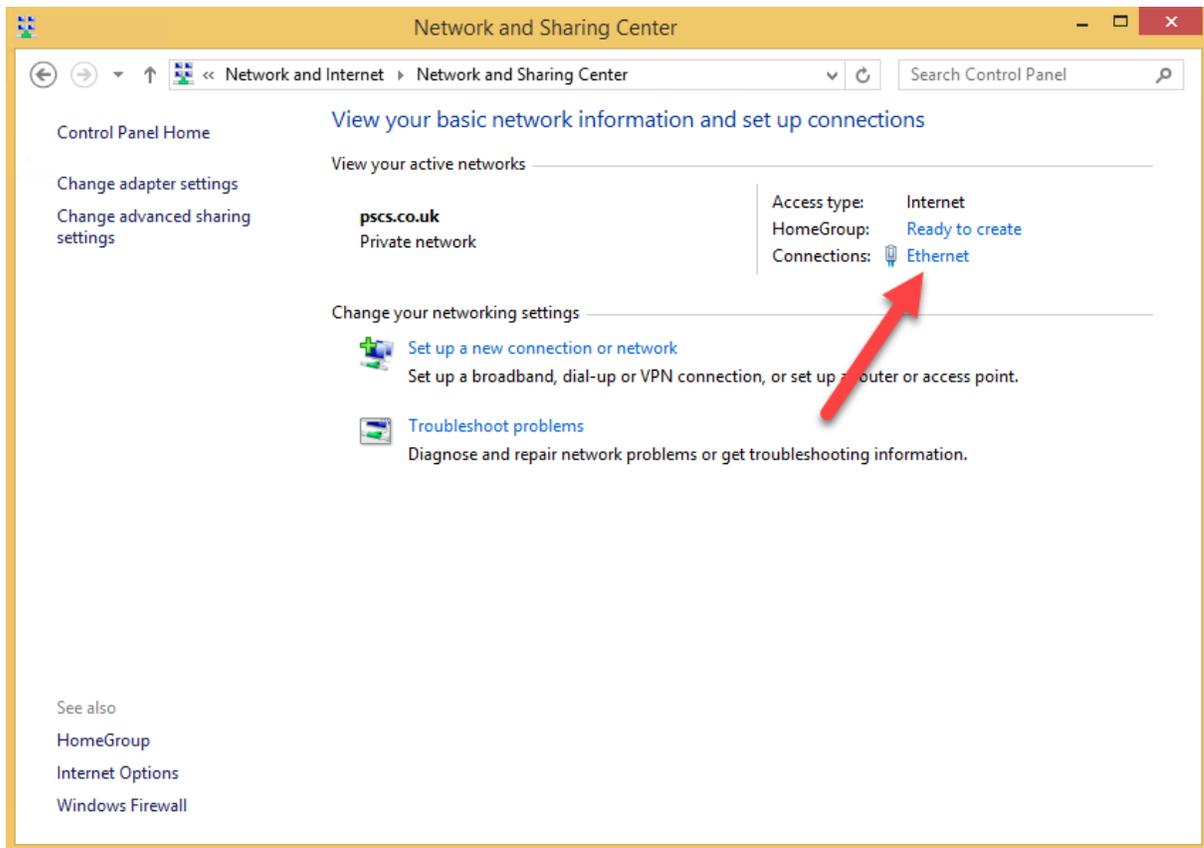
When setting up email clients to connect to VPOP3, you need to know the IP address of your VPOP3 server. You should also make sure that the VPOP3 computer always has the same IP address.

Determining the VPOP3 computer's IP address for LAN access

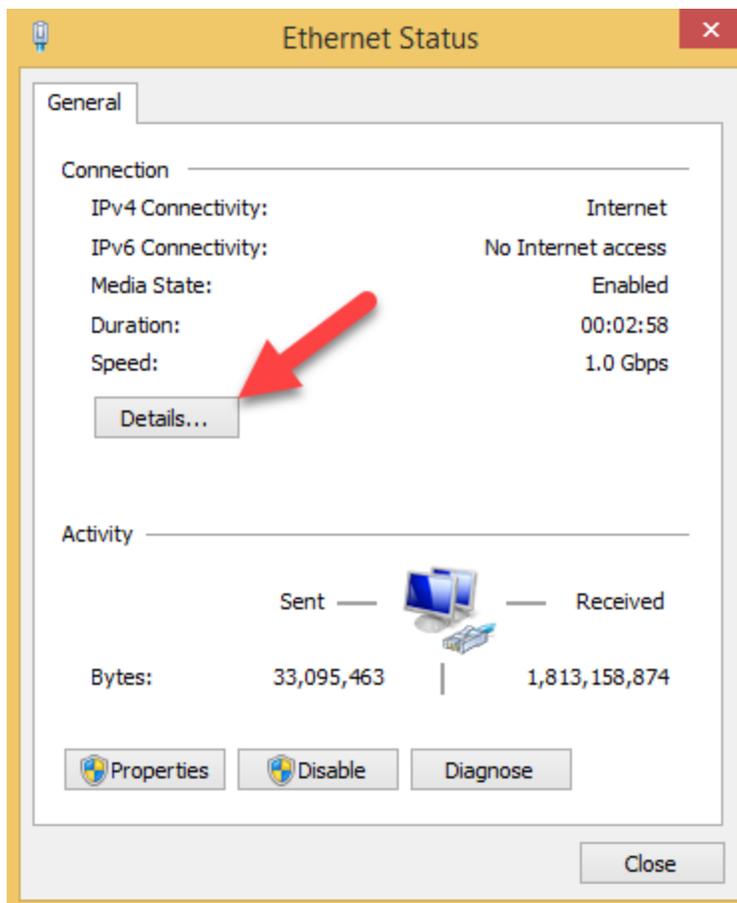
Go to the Windows Control Panel on the VPOP3 computer and **Network and Sharing Centre** or **View network status and tasks** depending on how you are viewing the Control Panel icons.



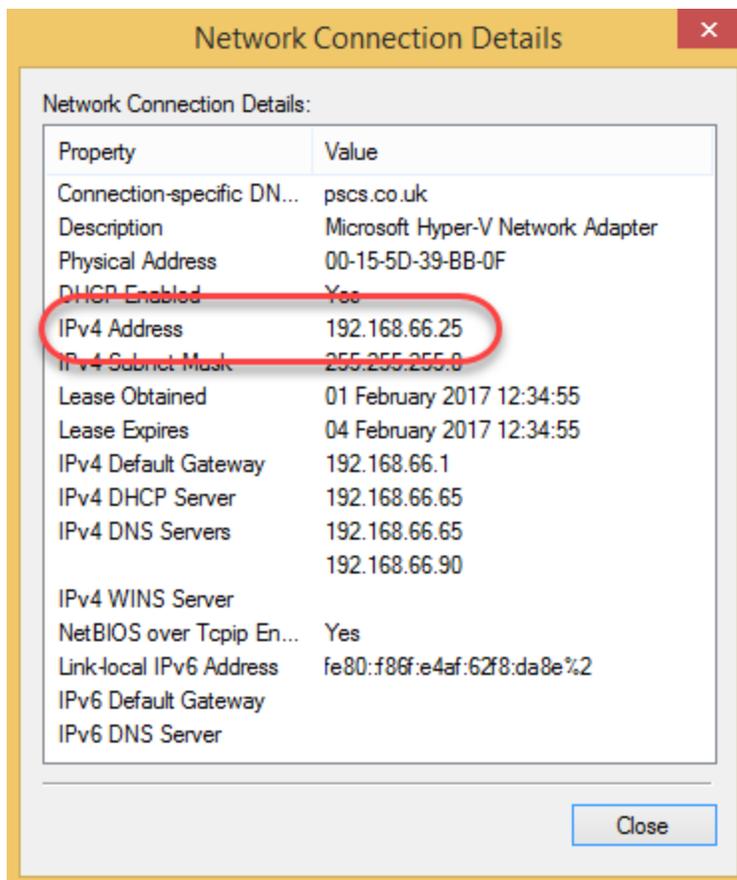
Click on the text next to **Connections**. It often says **Ethernet** here, but the text could be different depending on your computer's configuration.



Press the **Details** button.



Look at the value of the **IPv4 Address** field. This is the IP address of the VPOP3 computer.



Determining the VPOP3 computer's IP address for access across the Internet

If you want to access VPOP3 from across the Internet, then you need to access it using the external IP address of your Internet connection.

If you have a static IP address from your Internet provider, then they should have told you your static IP address, or you can search for **What is my IP address** on an Internet search engine.

If you do not have a static IP address from your Internet provider, then you will either need to get one, or use a 'Dynamic DNS service' which will link a name to your dynamic IP address. The Dynamic DNS service you choose will help you set this up.

Once you know the IP address you need to [set up VPOP3 and your router/firewall to allow access from outside your local network](#).

Fixing the VPOP3 computer's IP address on the LAN

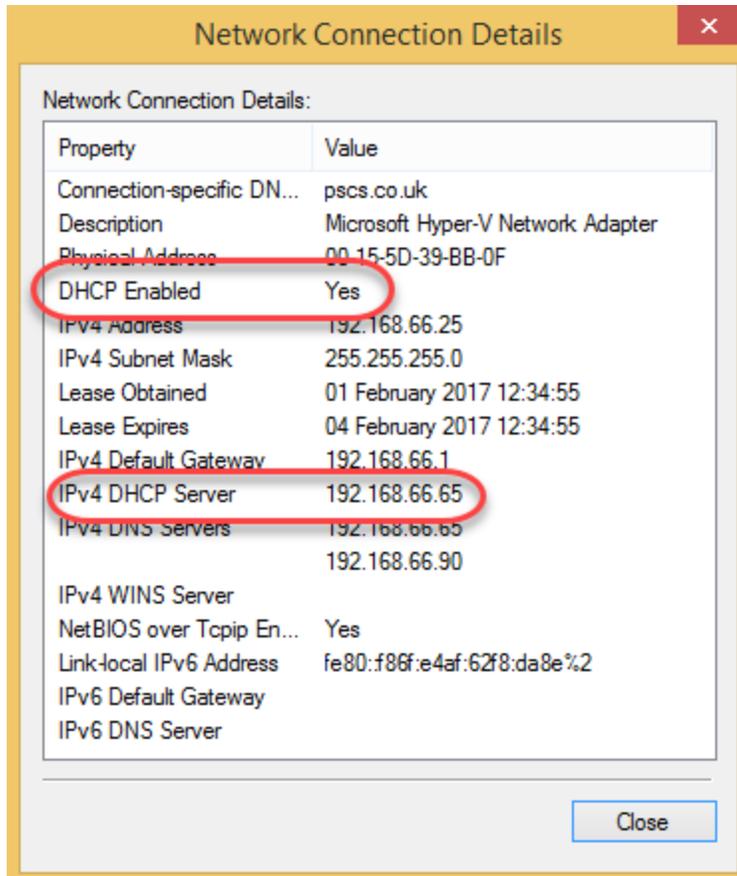
For reliable operation, the VPOP3 computer's IP address should never change. Users' computers will be trying to access it on a certain IP address, and if the IP address changes, then the users' computers will not be able to contact it.

On most networks nowadays, computers obtain their IP addresses using a system called DHCP (Dynamic Host Configuration Protocol). There will probably be a DHCP server on your network (eg a router or a network server), and when a computer/device is turned on, it asks that server for the network configuration, including which IP address it should use. If this is used, unchanged, on the computer

running VPOP3, then it may mean that when the computer is restarted, it will have a different IP address, and users' computers will be unable to collect or send email.

So, you should make sure that the VPOP3 computer always has the same IP address. If you are in a business, then this is something that your network administrator should do, so if that is not you, you should coordinate with that person to avoid causing problems.

You can tell if your computers are using DHCP and where the DHCP server is by looking at the network status. If you follow the instructions above for finding the local network IP address, in the **Details** window, there will be information about the DHCP status.



In the above screenshot, this shows that this computer has received its IP address from a DHCP server (**DHCP Enabled - Yes**) and that the DHCP server used was at IP address **192.168.66.65 (IPv4 DHCP Server - 192.168.66.65)**.

Using DHCP reservation

The recommended way to fix the computer's IP address is to use something called 'DHCP reservation'. This tells the DHCP server that whenever it receives a request from a certain network adapter, then it should provide the same IP address. This means that a certain computer will always have the same IP address (unless the network adapter is changed).

How you do this depends on what DHCP server you are using.

Some instructions for common DHCP servers are below:

- [Windows Server DHCP service](#)

- [Linux DHCPd](#) - (example)
- [D-Link Routers](#)
- [Netgear Routers](#)
- [Draytek Routers](#)

If your router is not shown above, then searching on the Internet for something like "<name of router> dhcp reservation" will probably find relevant instructions.

Using network settings

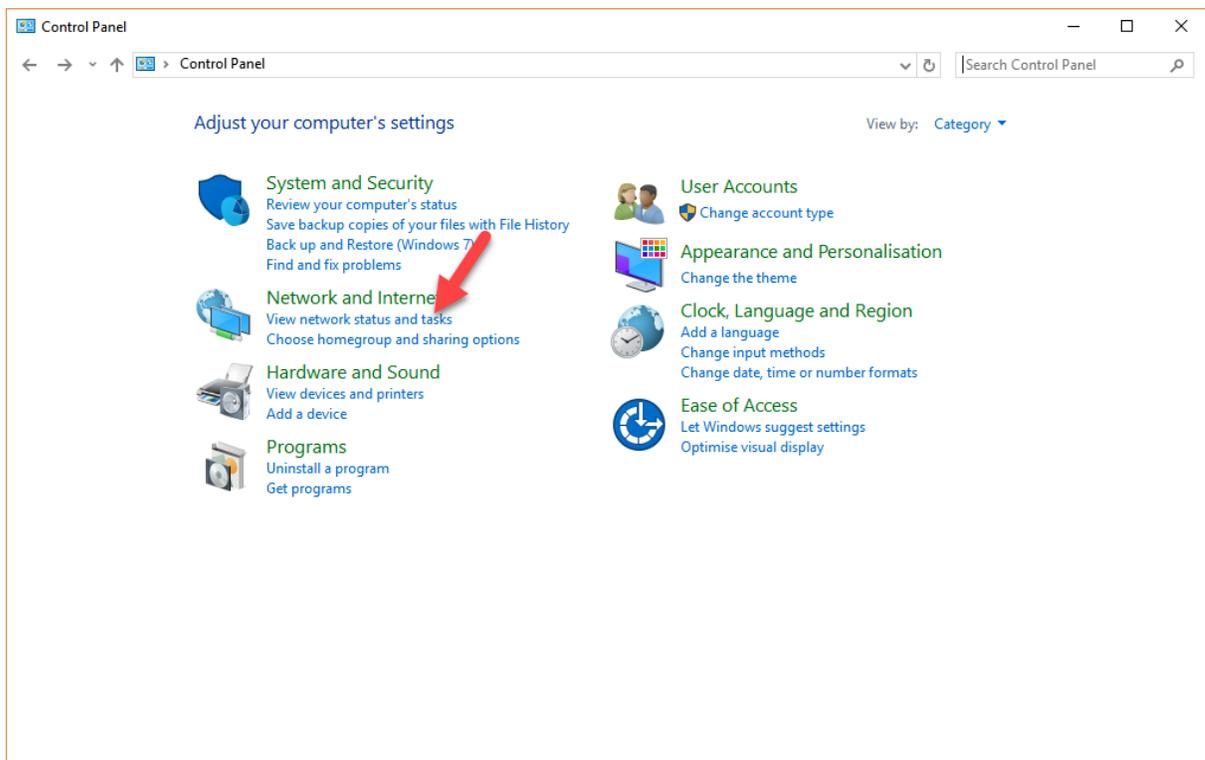
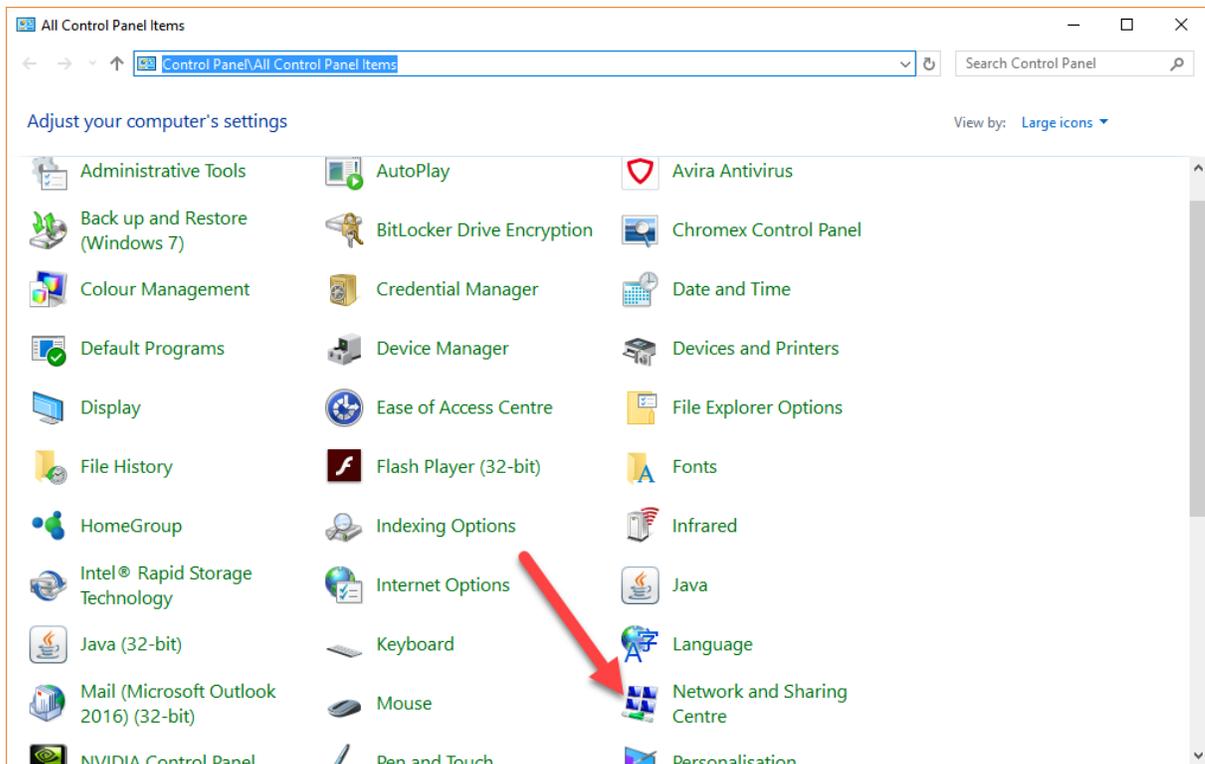
If you do not have a local DHCP server, then you can set the IP address manually. You can also do this if your DHCP server does not support reservations.

You must first choose a suitable IP address. This is a complicated subject, so we cannot include all possibilities. In a simple case, typically, it must be in the same subnet as the router, but be an address which is not used elsewhere. For instance, if your router is 192.168.1.1, and the subnet mask is 255.255.255.0, then your router's subnet has address 192.168.1.1 to 192.168.1.254. Choose an IP address in this range which is not used anywhere else. This can be hard to do if you do not have adequate network documentation...

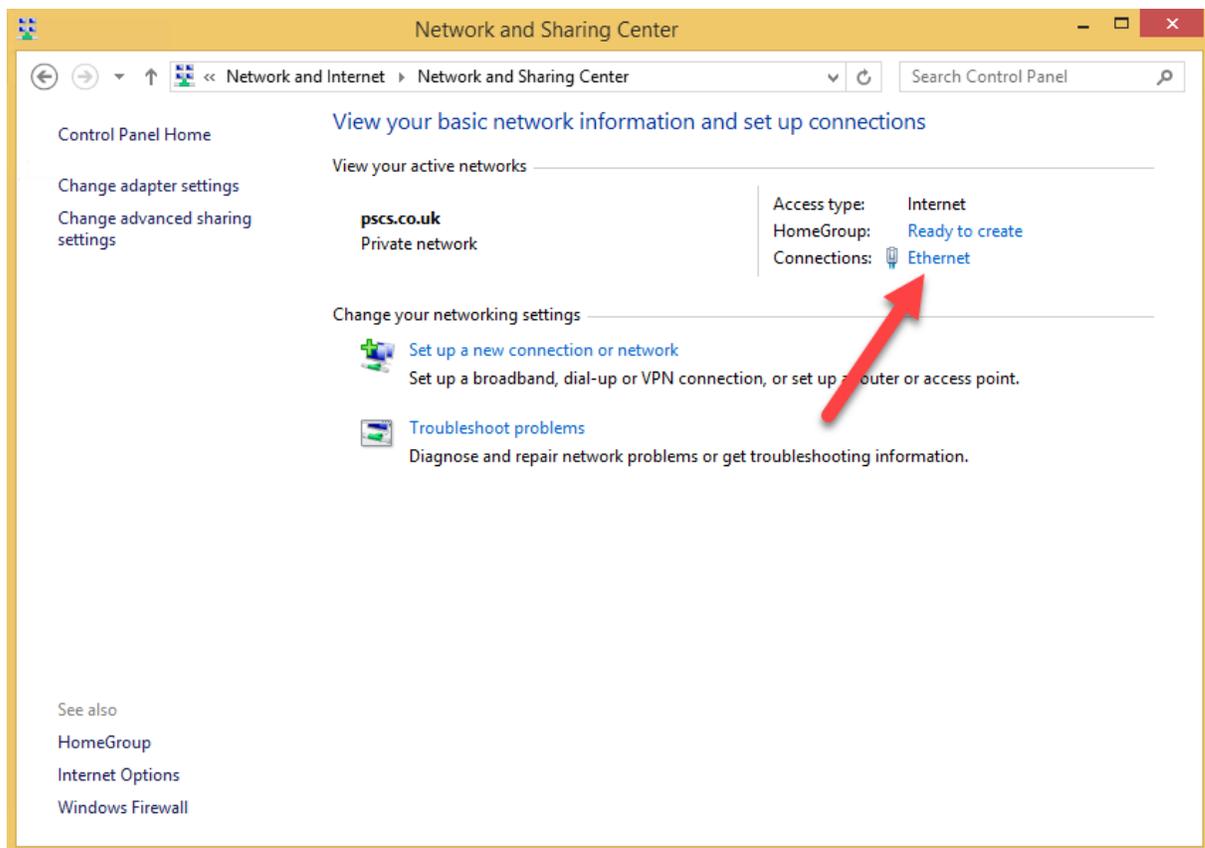
If you have a DHCP server which does not support reservations, then you can probably use an IP address which is outside the DHCP server's "address pool" and which is not used by other fixed items such as your router.

Once you have chosen the IP address to use you need to set it in Windows.

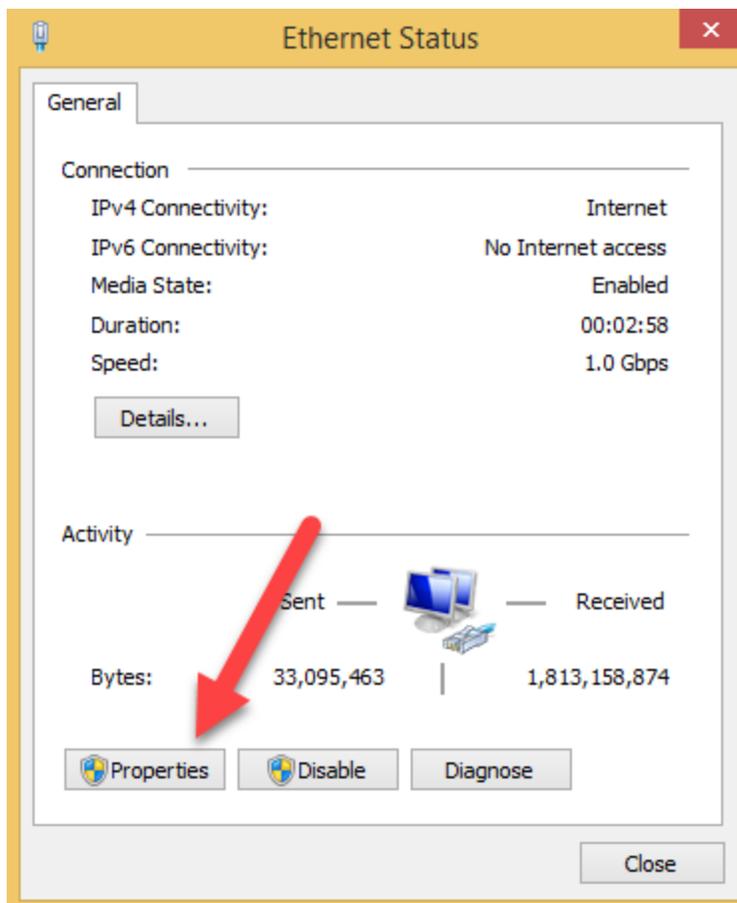
Go to the Windows Control Panel on the VPOP3 computer and **Network and Sharing Centre** or **View network status and tasks** depending on how you are viewing the Control Panel icons.



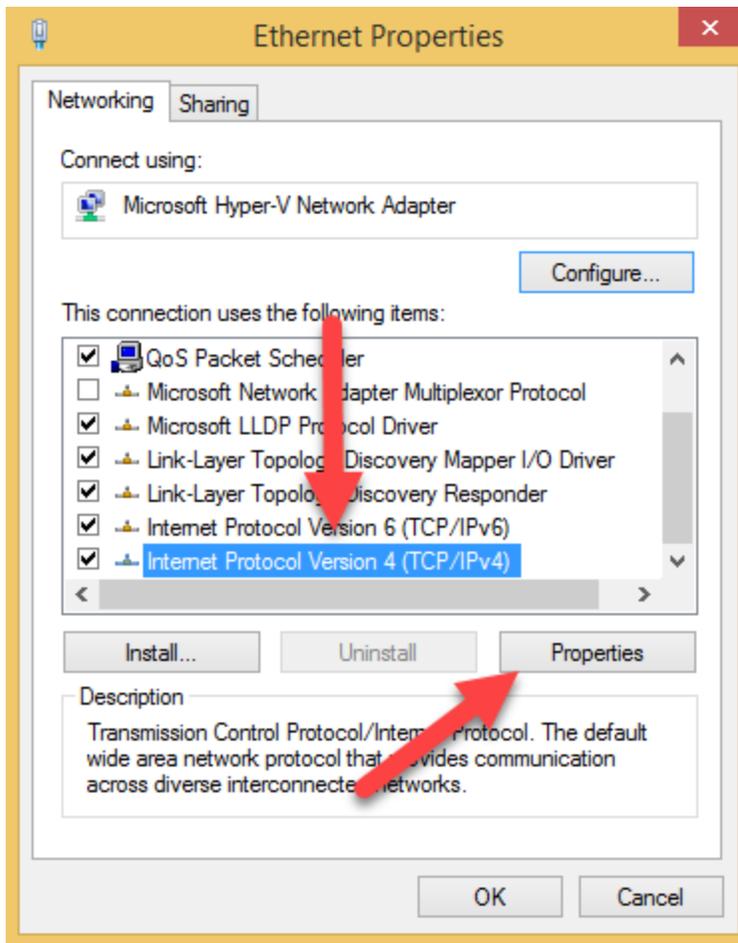
Click on the text next to **Connections**. It often says **Ethernet** here, but the text could be different depending on your computer's configuration.



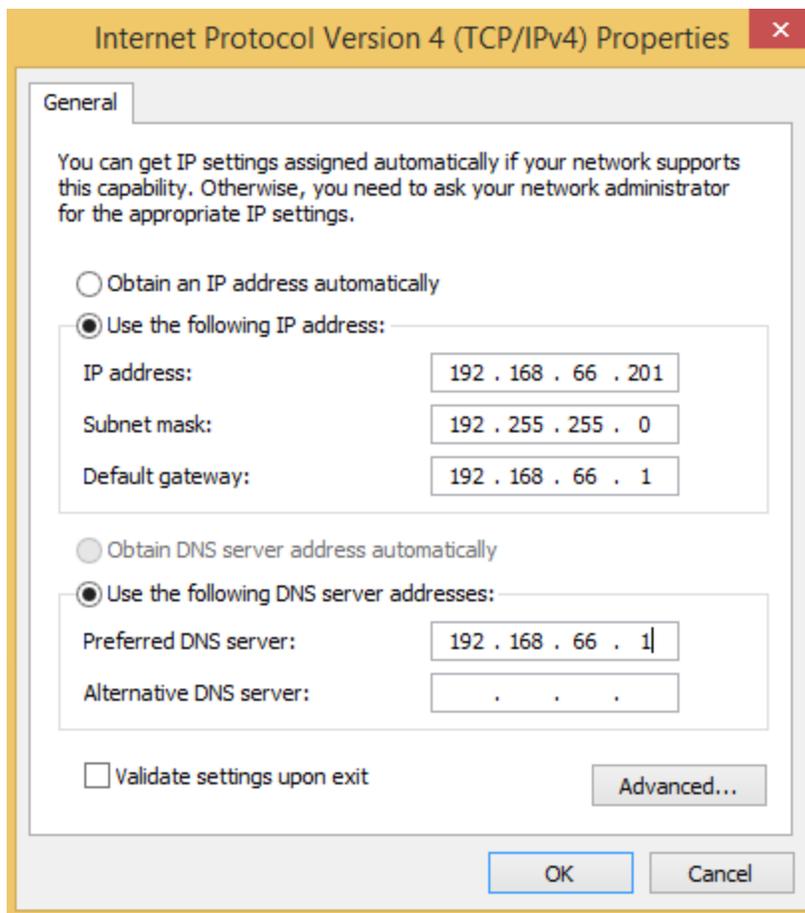
Press the **Properties** button.



Select the **Internet Protocol Version 4 (TCP/IPv4)** item, and press **Properties**.

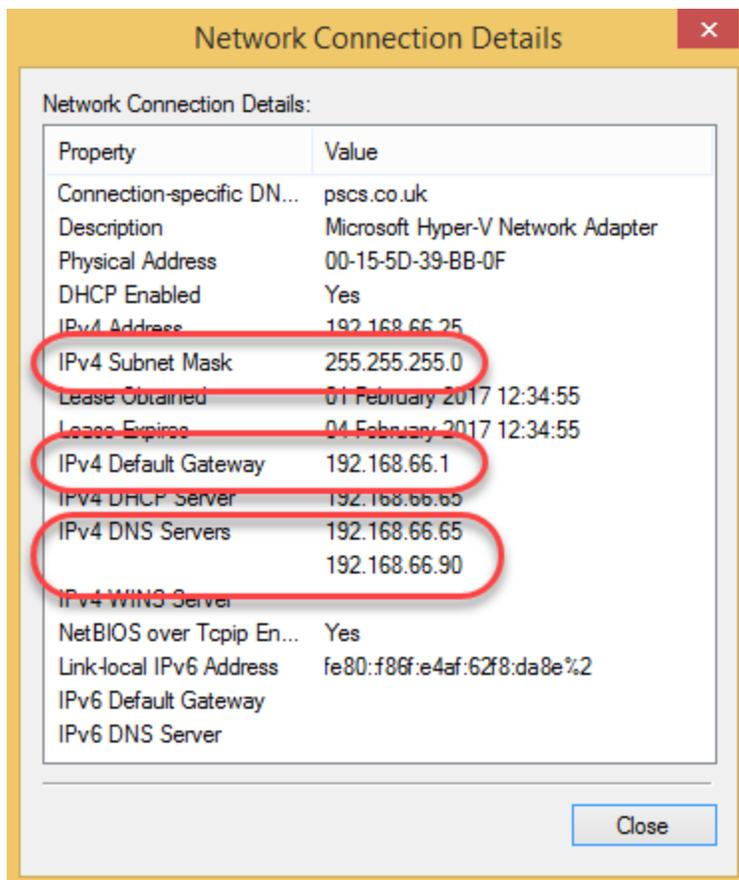


Now, enter the details



Enter the chosen IP address in the **IP address** box.

The **Subnet mask**, **Default gateway**, and **DNS servers** can be discovered from the network details which can be obtained as described above.



2.5.2 emClient

These instructions are for eM Client 6.0 but may be useful for other versions of eM Client.

In Outlook, go to **Tools -> Accounts** and select **Mail**

New Account ×

Set up an account

 Automatic Setup ▲

Enter your email and password and press Start Now.

Email:

Password: 

 Mail ▼

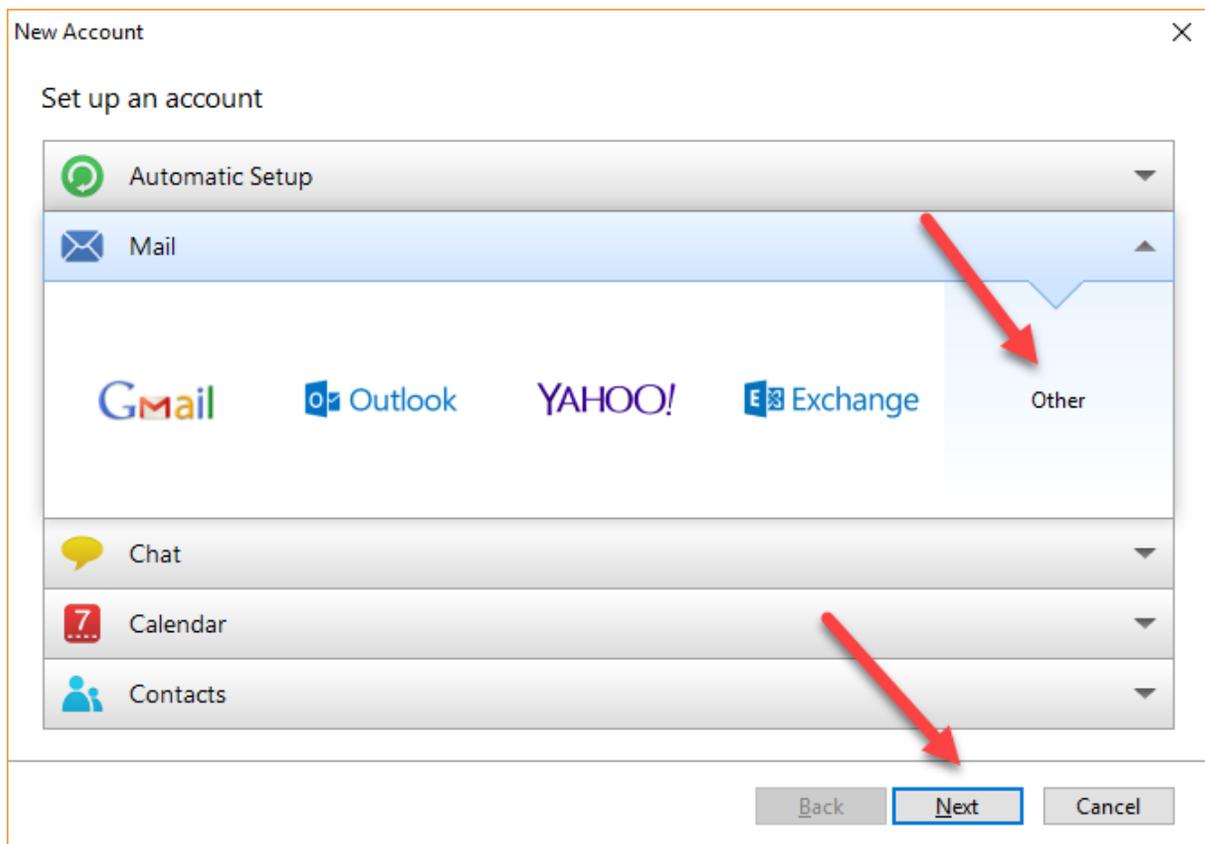
 Chat ▼

 Calendar ▼

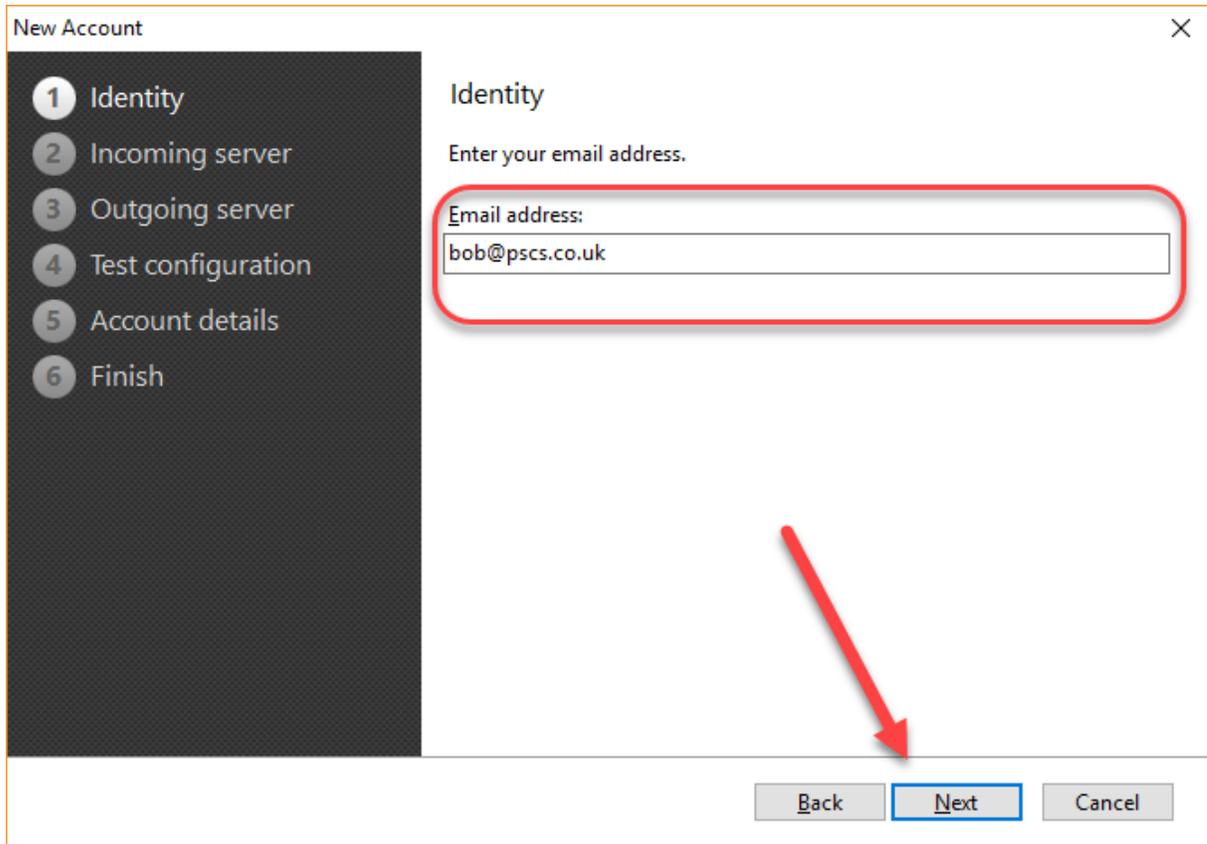
 Contacts ▼

Back Next Cancel

Select **Other**, then **Next**



Enter your email address and press **Next**.



The screenshot shows a 'New Account' dialog box with a sidebar on the left containing six steps: 1 Identity, 2 Incoming server, 3 Outgoing server, 4 Test configuration, 5 Account details, and 6 Finish. The 'Identity' step is selected. The main area is titled 'Identity' and contains the instruction 'Enter your email address.' Below this is a text input field labeled 'Email address:' containing the text 'bob@psecs.co.uk'. A red rounded rectangle highlights the input field. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'. A red arrow points to the 'Next' button.

Select POP3 or IMAP as appropriate ([POP3](#) if you are using VPOP3 Basic or are using VPOP3 Enterprise and want to use POP3, IMAP if using VPOP3 Enterprise and want to use [IMAP4](#)).

In the **Incoming server** box enter the DNS name or [IP address](#) of the VPOP3 computer.

In the **User name** box enter the VPOP3 username defined in the [Users](#) list (not the full email address).

In the **Password** box enter the VPOP3 password defined in the Users list.

Press **Next**

The screenshot shows a 'New Account' dialog box with a sidebar on the left containing six steps: 1 Identity, 2 Incoming server, 3 Outgoing server, 4 Test configuration, 5 Account details, and 6 Finish. The 'Incoming server' step is highlighted. The main area is titled 'Incoming server' and contains the following fields and options:

- Radio buttons for 'POP3' (selected) and 'IMAP'.
- Text input for 'Incoming server:' with the value '192.168.0.20'.
- Text input for 'User name:' with the value 'bob'.
- Text input for 'Password:' with masked characters '.....'.

At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

Leave the Outgoing Server settings as they are (eM client will copy them from the previous page, which is correct). Make sure that **Outgoing server doesn't require authentication is not checked**.

Press **Next**

The screenshot shows a 'New Account' dialog box with a sidebar on the left containing six steps: 1 Identity, 2 Incoming server, 3 Outgoing server (highlighted), 4 Test configuration, 5 Account details, and 6 Finish. The main area is titled 'Outgoing server' and contains the following text and fields:

Enter the name of your outgoing mail server (for example "mail.example.com").

Outgoing server:

Enter your user name (if it differs from the incoming user name).

User name:

Password:

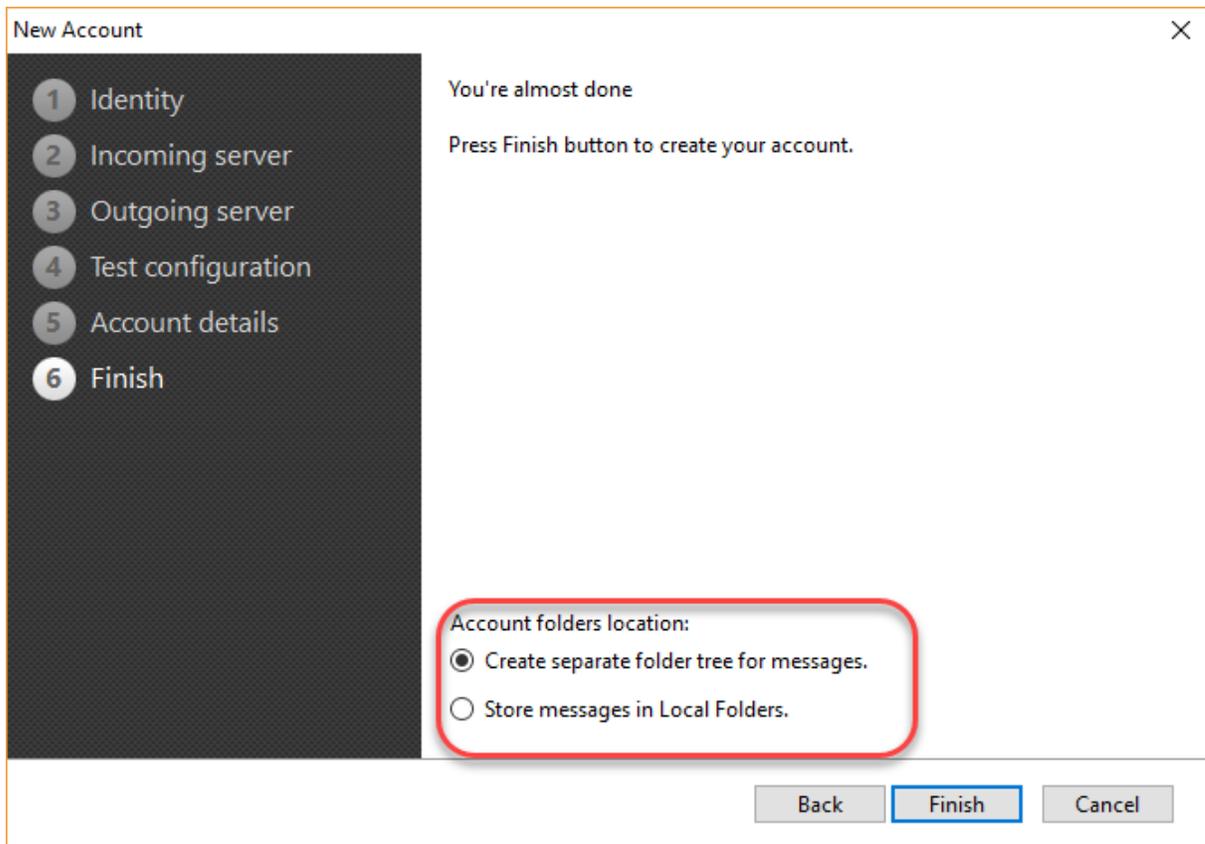
Outgoing server doesn't require authentication

At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a blue border and a red arrow pointing to it), and 'Cancel'.

Press **Next** to test the account settings, **Next** to enter your name and account name and **Next** again.

If you chose **POP3** as the incoming server type, then you have the option of having eM Client store your messages from this account in the general **Local Folders** area, or keeping them separate (**Create separate folder tree for messages**).

If you chose **IMAP** then this isn't an option because they will always be kept separate. This is because eM Client will show what is stored on the server, and if that is mixed in with messages which aren't stored on the server, it would be very confusing.

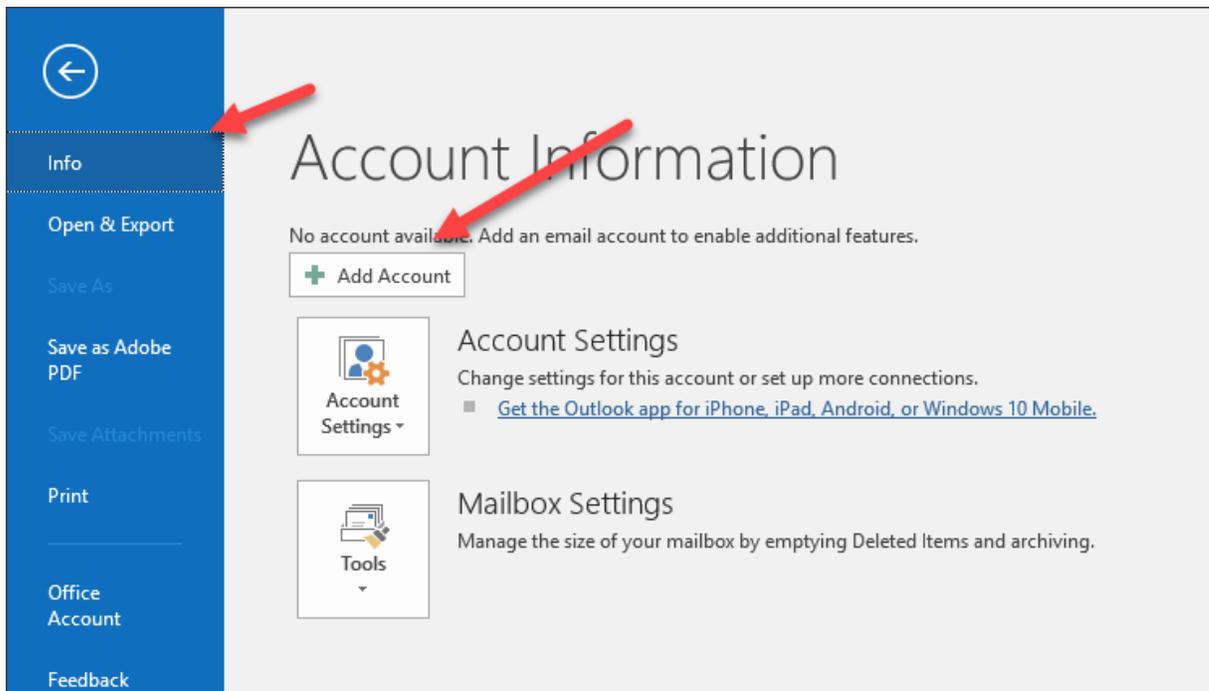


Press **Finish** to add the account.

2.5.3 Microsoft Outlook 2016

These instructions are for Microsoft Outlook 2016 but may be useful for other versions of Outlook.

In Outlook, go to **File -> Info** and click on **Add Account**



In the **Auto Account Setup** page of the Add Account wizard, choose **Manual setup or additional server types** and press **Next**.

Add Account ✕

Auto Account Setup
Manual setup of an account or connect to other server types. 

Email Account

Your Name:
Example: Ellen Adams

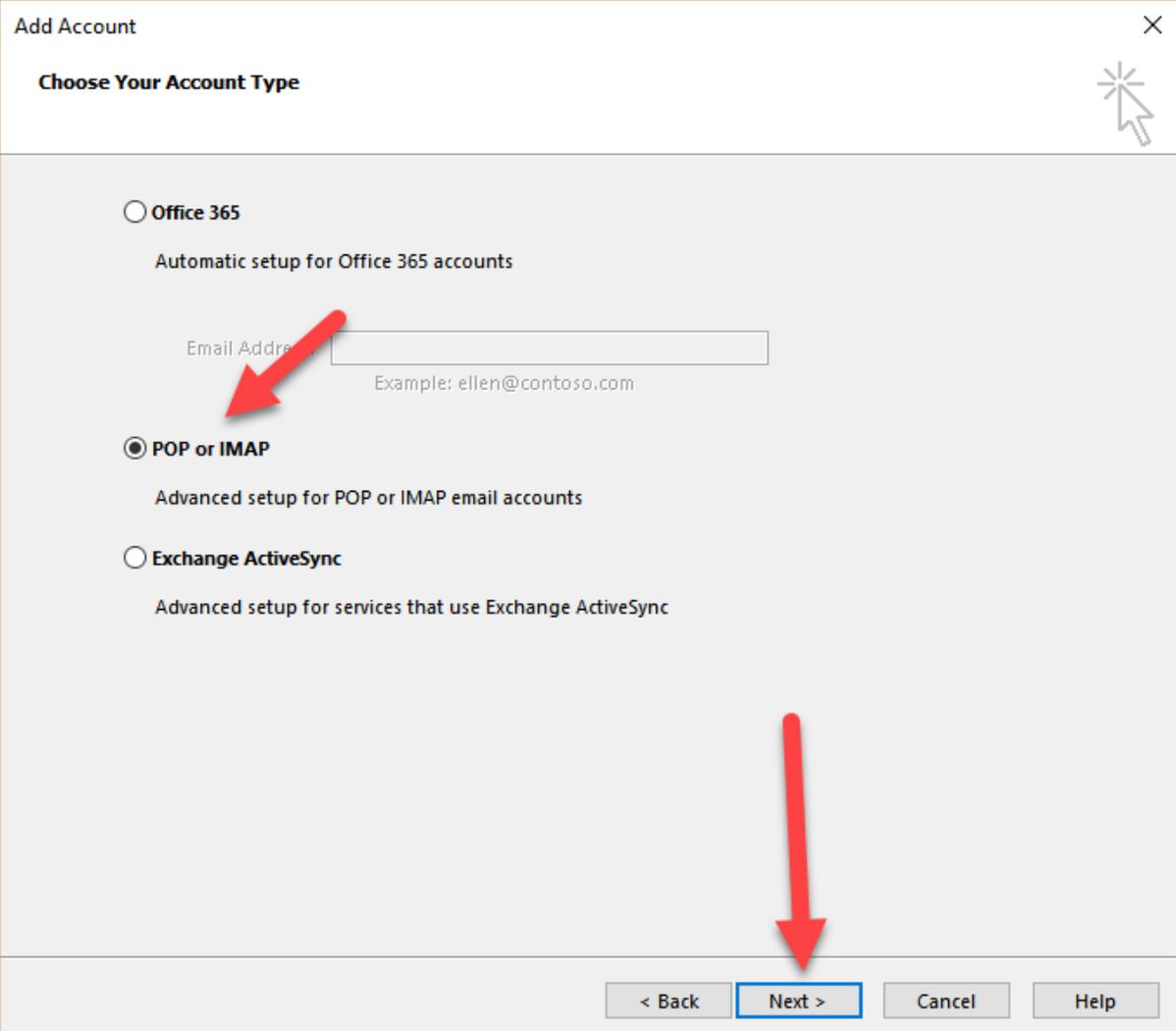
Email Address:
Example: ellen@contoso.com

Password:

Retype Password:
Type the password your Internet service provider has given you.

Manual setup or additional server types

In the **Choose Your Account Type** page, choose **POP or IMAP** and press **Next**.



The screenshot shows a window titled "Add Account" with a close button (X) in the top right corner. Below the title bar is the heading "Choose Your Account Type". There are three radio button options:

- Office 365
Automatic setup for Office 365 accounts
- POP or IMAP
Advanced setup for POP or IMAP email accounts
- Exchange ActiveSync
Advanced setup for services that use Exchange ActiveSync

Under the "Office 365" option, there is an "Email Address" label and a text input field. A red arrow points to the input field, which contains the example text "ellen@contoso.com".

At the bottom of the dialog, there are four buttons: "< Back", "Next >" (highlighted with a blue border), "Cancel", and "Help". A red arrow points to the "Next >" button.

In the **POP3 and IMAP Account Settings** page, enter your server & account details.

Add Account [Close]

POP and IMAP Account Settings
Enter the mail server settings for your account.

User Information

Your Name:

Email Address:

Server Information

Account Type: [v]

Incoming mail server:

Outgoing mail server (SMTP):

Logon Information

User Name:

Password:

Remember password

Require logon using Secure Password Authentication (SPA)

Test Account Settings

We recommend that you test your account to ensure that the entries are correct.

Automatically test account settings when Next is clicked

Mail to keep offline: All

< Back **Next >** Cancel Help

In **Your Name** put your name.

In **Email Address** put your email address.

In **Account Type** choose IMAP or POP as appropriate. If you have [VPOP3 Basic](#), then you must put POP. If you have VPOP3 Enterprise, then we recommend you choose IMAP, but there may be situations where you want to use POP instead. If more than one computer/device will be accessing your email, then IMAP is strongly recommended so that your email is synchronised between devices.

In **Incoming mail server** enter the [IP address or name](#) of the computer running VPOP3.

In **Outgoing mail server** enter the IP address or name of the computer running VPOP3 (exactly like the **Incoming mail server** setting).

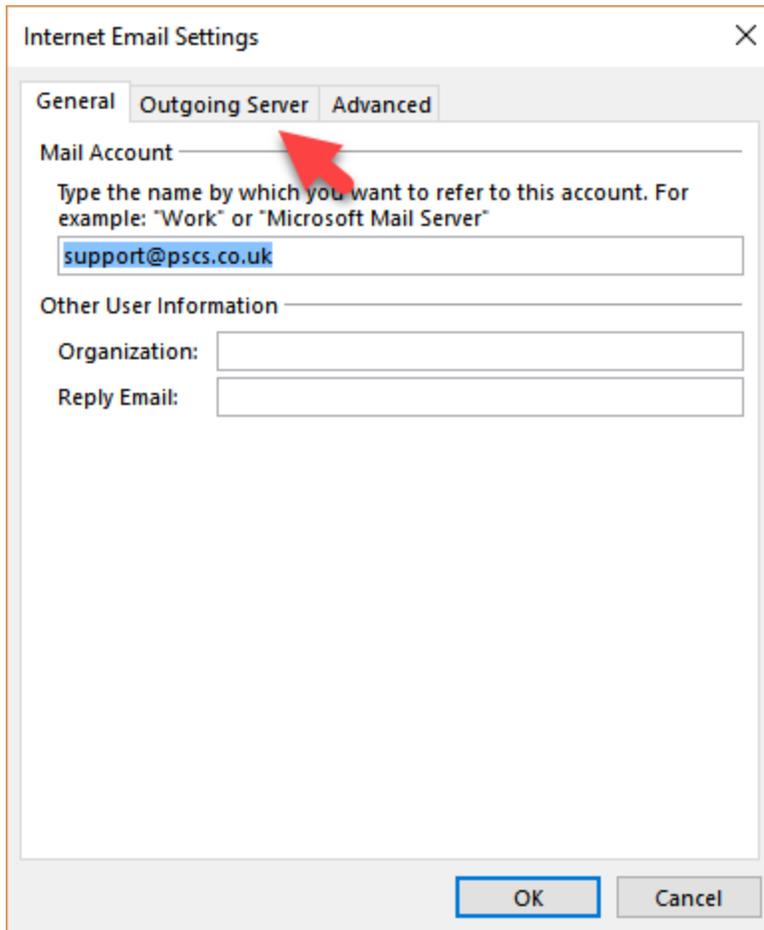
In **User Name** enter the user name exactly as [you have defined it within VPOP3](#). Note that when using VPOP3, you should enter the user name here, *not* the full email address.

In **Password** enter the password exactly as you have defined it within VPOP3.

Check the **Remember password** box.

Ensure that the **Require logon using Secure Password Authentication** box is *not* checked.

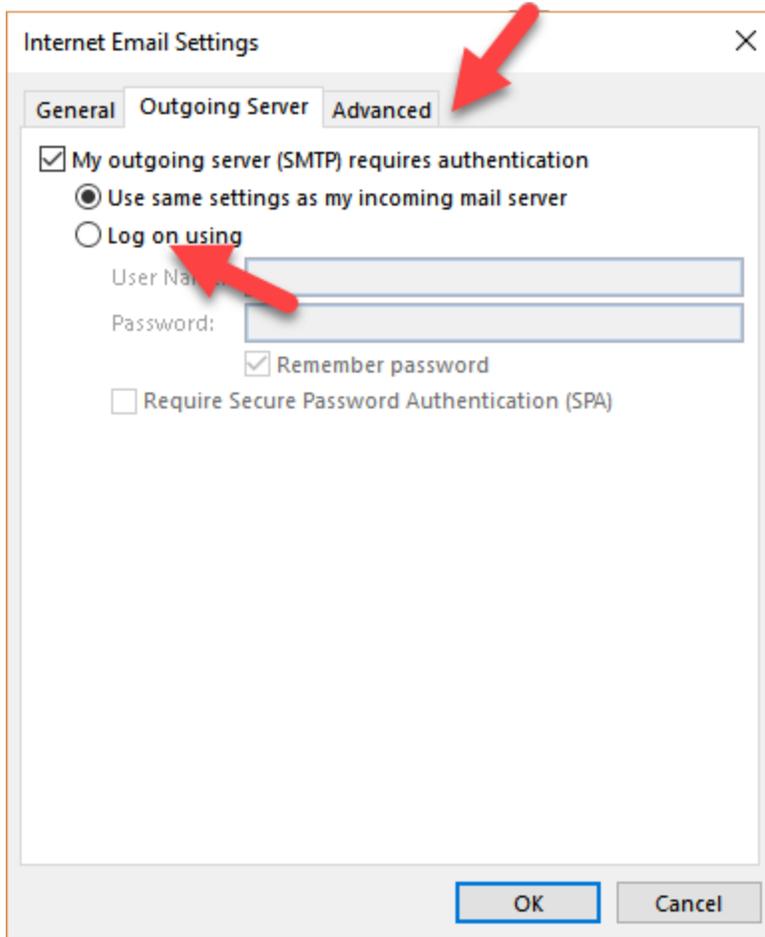
Press the **More Settings...** button.



The screenshot shows a dialog box titled "Internet Email Settings" with a close button (X) in the top right corner. It has three tabs: "General", "Outgoing Server", and "Advanced". The "General" tab is selected. Under "Mail Account", there is a text box containing "support@psecs.co.uk" with a red arrow pointing to it. Below this is the instruction: "Type the name by which you want to refer to this account. For example: 'Work' or 'Microsoft Mail Server'". Under "Other User Information", there are two empty text boxes labeled "Organization:" and "Reply Email:". At the bottom right, there are "OK" and "Cancel" buttons.

On the **General** tab, enter settings as you wish. Normally you can leave them at the defaults. If you want to change the name of the Account in Outlook (for instance, to make it clear that this is the account which communicates with VPOP3) then this is the place to do it.

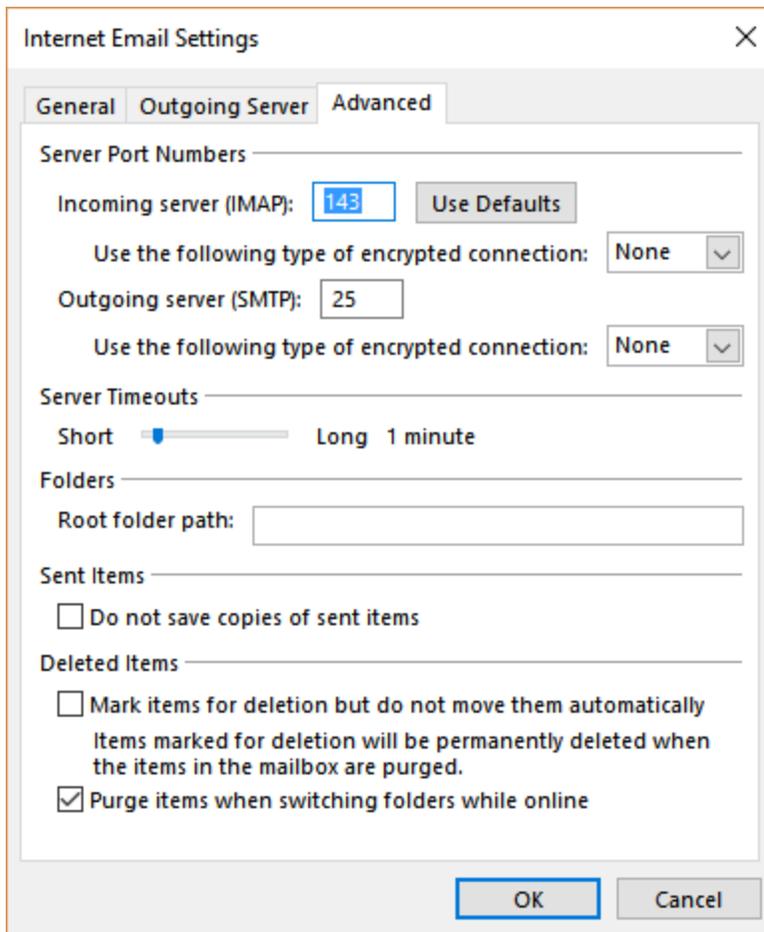
Select the **Outgoing Server** tab.



Select **My outgoing server (SMTP) requires authentication** and **Use the same settings as my incoming mail server**.

Select the **Advanced** tab.

If you are using IMAP for the incoming mail type, then you will see a tab like this:



Check the server port numbers are correct. The defaults are usually correct, but if you have changed the [VPOP3 server ports](#) then you may need to change them here.

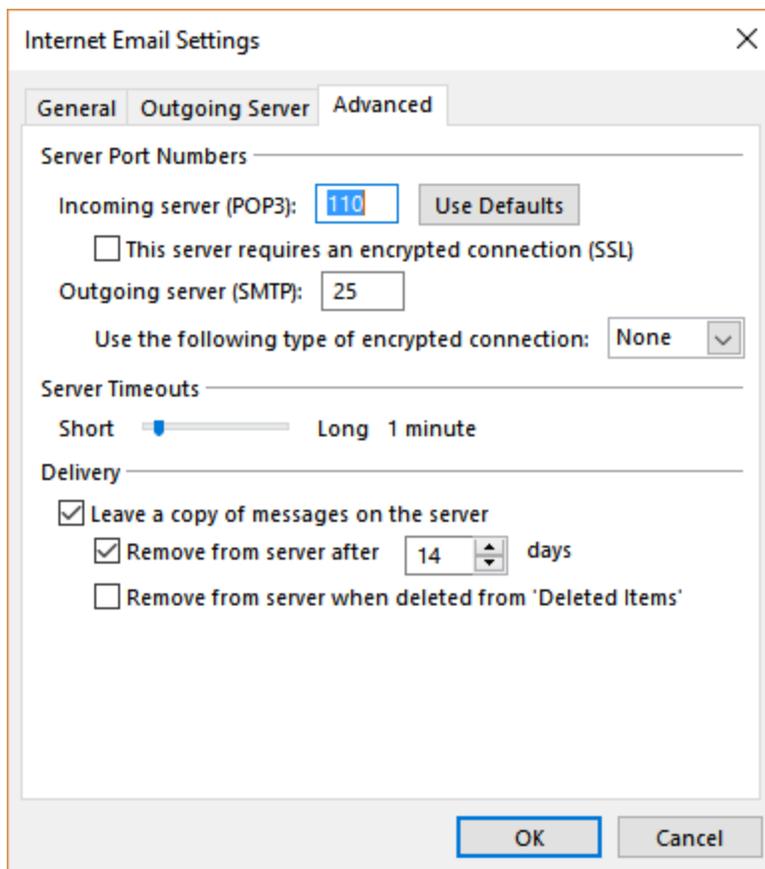
If you have set up [server session encryption](#) in VPOP3 (VPOP3 Enterprise only), then select the appropriate value for the encryption options here. **TLS** here is the same as **STARTTLS** in VPOP3 and **SSL** here is the same as **SSL** in VPOP3.

We recommend increasing the **Server Timeouts** value. The Internet standards recommend a much longer timeout than 1 minute, and if the timeout is too short it can lead to duplicated messages.

The **Root Folder Path** should be blank for use with VPOP3.

The other options can be set as you wish.

If you are using POP for the incoming mail type, then the Advanced tab will be like this:



Check the server port numbers are correct. The defaults are usually correct, but if you have changed the [VPOP3 server ports](#) then you may need to change them here.

If you have set up [server session encryption](#) in VPOP3 (VPOP3 Enterprise only), then select the appropriate value for the encryption options here. **TLS** here is the same as **STARTTLS** in VPOP3 and **SSL** here is the same as **SSL** in VPOP3. Outlook currently only supports SSL encryption for POP3 sessions.

We recommend increasing the **Server Timeouts** value. The Internet standards recommend a much longer timeout than 1 minute, and if the timeout is too short it can lead to duplicated messages.

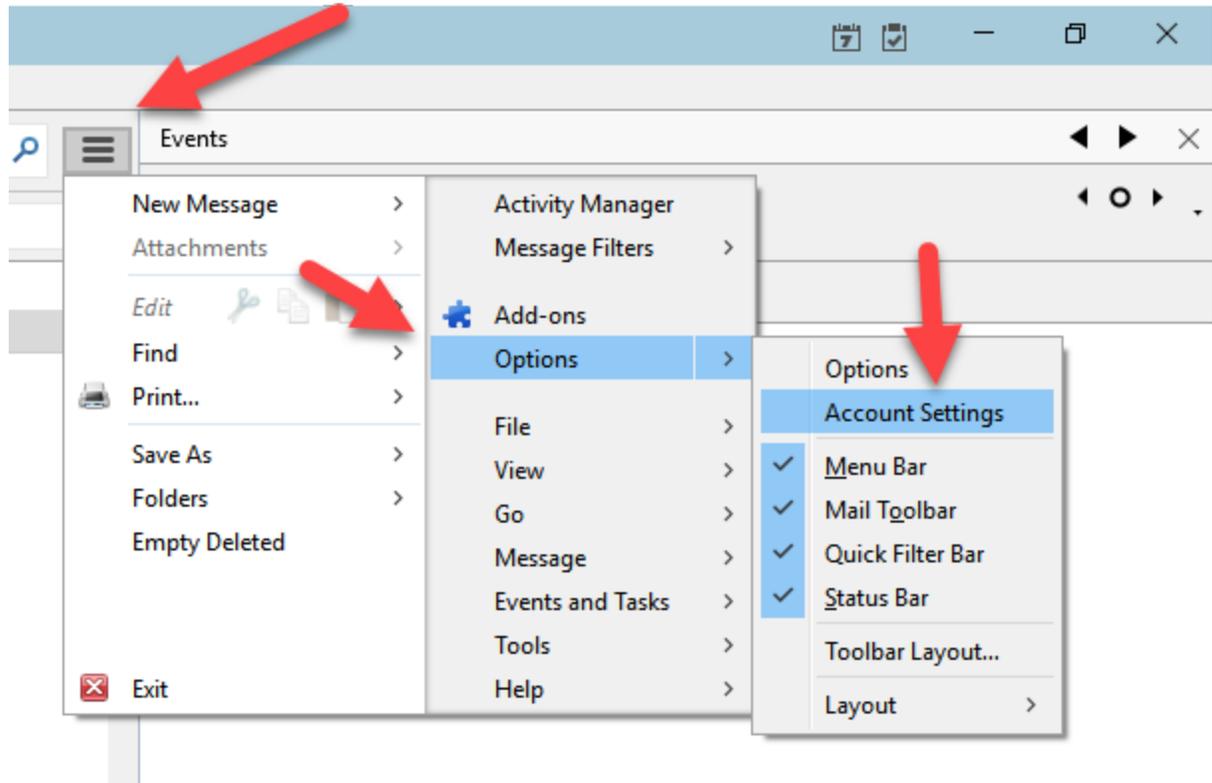
The other options can be set as you wish. The **Leave a copy of messages on the server** options tell Outlook to leave messages on the VPOP3 server after it has downloaded them.

- Close the **Internet Email Settings** window, and press **Next** for Outlook to test the connection settings and set up the account.

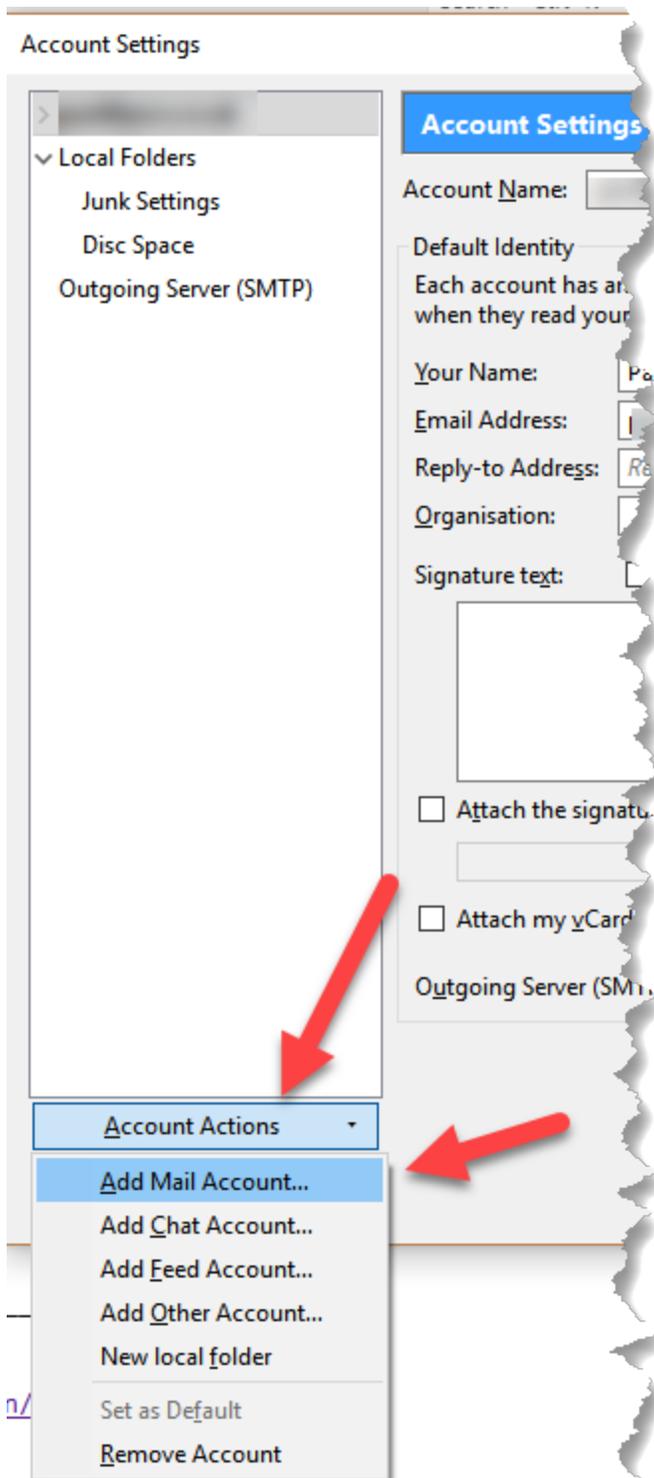
2.5.4 Mozilla Thunderbird

These instructions are for Mozilla Thunderbird 45.7 but will probably be similar for other versions.

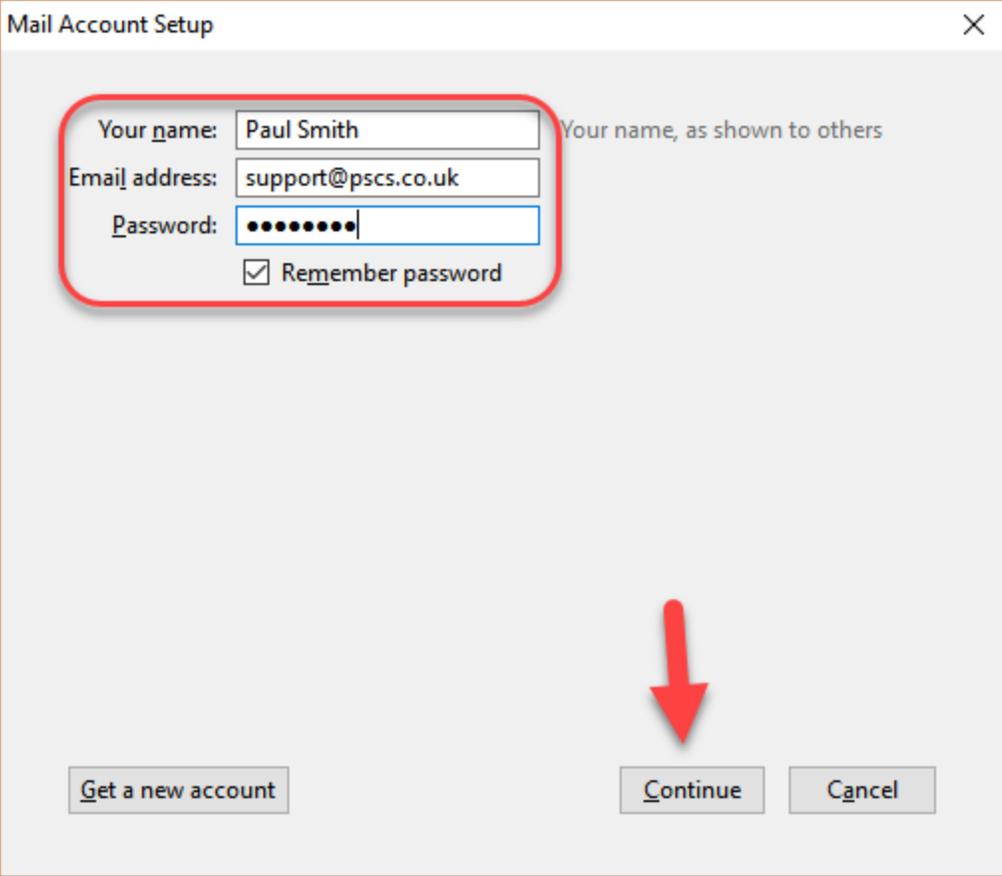
Click on the menu button, then **Options** -> **Account Settings**



Click **Account Actions** at the bottom of the **Account Settings** window, then **Add Mail Account**



On the next page enter your details



Mail Account Setup

Your name: Paul Smith Your name, as shown to others

Email address: support@psecs.co.uk

Password: ●●●●●●

Remember password

Get a new account

Continue Cancel

In **Your name** enter your name.

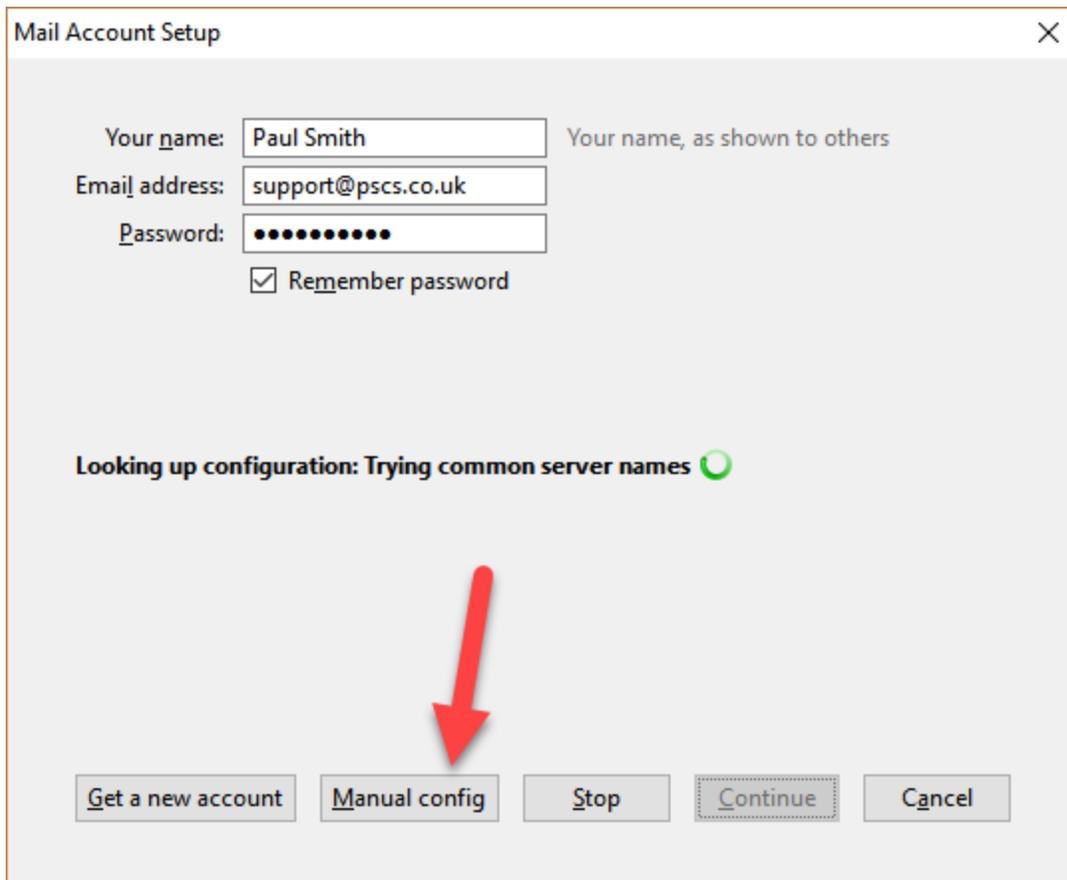
In **Email address** enter your email address.

In **Password** enter your password as defined in the VPOP3 [User](#) settings.

Make sure the **Remember password** box is checked.

Press the **Continue** button.

Thunderbird will now try to guess your server details. The chances are that it will fail, so you can press the **Manual config** button to make it skip the guess phase.



Mail Account Setup

Your name: Your name, as shown to others

Email address:

Password:

Remember password

Looking up configuration: Trying common server names 

If Thunderbird does manage to guess the correct details, then you can press **Done** to finish, or if it guesses the incorrect details, you can press the **Manual config** button at that stage to enter the server details manually.

Mail Account Setup

Your name: Your name, as shown to others

Email address:

Password:

Remember password

Configuration found by trying common server names

IMAP (remote folders) POP3 (keep mail on your computer)

Incoming: IMAP, mail.pscs.co.uk, STARTTLS

Outgoing: SMTP, mail.pscs.co.uk, STARTTLS

Username: support

On this page you can enter the server details

Mail Account Setup

Your name: Your name, as shown to others

Email address:

Password:

Remember password

	Server hostname	Port	SSL	Authentication
Incoming: IMAP	<input type="text" value="192.168.66.70"/>	<input type="text" value="Auto"/>	<input type="text" value="Autodetect"/>	<input type="text" value="Autodetect"/>
Outgoing: SMTP	<input type="text" value="192.168.66.70"/>	<input type="text" value="Auto"/>	<input type="text" value="Autodetect"/>	<input type="text" value="Autodetect"/>

Username: Incoming: Outgoing:

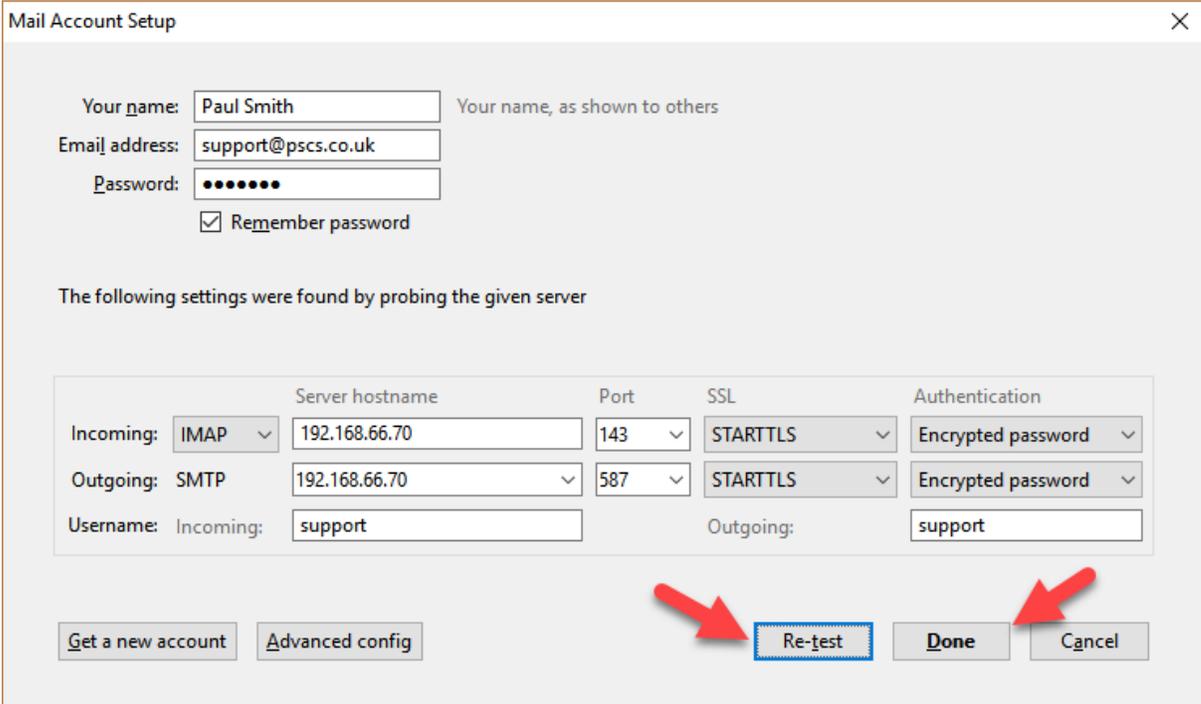
On the **Incoming** line, select whether Thunderbird should use IMAP4 or POP3. If you have [VPOP3 Basic](#), then you must put POP3. If you have VPOP3 Enterprise, then we recommend you choose IMAP, but there may be situations where you want to use POP3 instead. If more than one computer/device will be accessing your email, then IMAP is strongly recommended so that your email is synchronised between devices.

In the **Server hostname** column, enter the [IP address or name of the computer running the VPOP3 software](#) for both the **Incoming** and **Outgoing** servers.

Usually you can leave **Port**, **SSL** and **Authentication** as **Autodetect** and Thunderbird will try the most common settings to find ones which work.

On the **Username** row, put your username as specified in the [VPOP3 User settings](#) for both **Incoming** and **Outgoing**. Note that this is just the username, not a full email address.

Press the **Re-test** button to have Thunderbird test the settings and complete the **Autodetect** options.



Mail Account Setup

Your name: Your name, as shown to others

Email address:

Password:

Remember password

The following settings were found by probing the given server

	Server hostname	Port	SSL	Authentication
Incoming: IMAP	<input type="text" value="192.168.66.70"/>	<input type="text" value="143"/>	<input type="text" value="STARTTLS"/>	<input type="text" value="Encrypted password"/>
Outgoing: SMTP	<input type="text" value="192.168.66.70"/>	<input type="text" value="587"/>	<input type="text" value="STARTTLS"/>	<input type="text" value="Encrypted password"/>
Username: Incoming:	<input type="text" value="support"/>	Outgoing:	<input type="text" value="support"/>	

Assuming that completes OK, press the **Done** button

3 General Concepts and Terms

This section of the documentation defines and describes some terms used elsewhere in the documentation.

It can be useful to read through this section as it may help understand the concepts used in the operation of VPOP3.

3.1 Which programs do what

The VPOP3 software uses several programs. This section gives a basic description of the main programs

The VPOP3 Software itself

The VPOP3 software itself is *VPOP3.EXE*. This software has no user interface itself, so if you run it, you will not see anything appear on the screen, taskbar or task tray. The only place you will see it is in the *Processes* tab in Windows Task Manager (you may have to *Show Processes For All Users*).

The fact that VPOP3 is invisible can confuse some people, thinking that the software has not started, but it could well be running, especially if you see it in the *Processes* tab in Task Manager.



Upgrade Tip

In VPOP3 v1.x, you could run *VPOP3.EXE* to access the settings, now this won't do anything.

Instead, you should either right-click the [Status Monitor](#) and choose *VPOP3 Settings*, or go to *Start » Programs » VPOP3 » Configure VPOP3*

In the current versions of VPOP3, if you try to run VPOP3 several times, any instances after the first should automatically terminate once they detect another copy running.

The VPOP3 Status Monitor

The VPOP3 status monitor is a small program (*VPOP3STATUS.EXE*) which communicates with VPOP3 using TCP/IP and displays an icon () in the Windows task tray. This icon is the way most VPOP3 users access the VPOP3 status and settings.

For more information, see [this article](#).

The VPOP3 Service Controller

If you run VPOP3 as a service (recommended), then a small program called *VPOP3_SVC.EXE* will run, this talks to the Windows Service Manager and controls *VPOP3.EXE* appropriately. *VPOP3_SVC.EXE* will also automatically restart *VPOP3.EXE* if it detects it crashing unexpectedly.

For more information, see [this article](#).

The VPOP3DB Service

In the Windows Services list you will see a service called *VPOP3DB*. This is an instance of the PostgreSQL database server. It is called *VPOP3DB* in the services list to make it clear that it is part of *VPOP3*, so people hopefully will not uninstall or disable it accidentally.

It is possible to use *VPOP3* with a separate installation of PostgreSQL (possibly on a different PC) rather than the standard one, but this is an advanced topic.

VPOP3 requires access to the PostgreSQL service to run at all - all settings, users, messages etc are stored in the PostgreSQL database. By default, the *VPOP3* service is marked as "dependant" on the *VPOP3DB* service so Windows will start the database service first.

For more details about the PostgreSQL installation, see the [PostgreSQL installation details](#) topic.

3.2 Editions of VPOP3

VPOP3 is available in three editions, *VPOP3 Enterprise*, *VPOP3 Basic* and *VPOP3 Home User*.

VPOP3 Enterprise

VPOP3 Enterprise is the most feature-rich version of *VPOP3*. As well as [POP3](#) & [SMTP](#) support, this edition includes [IMAP4](#) support to allow mailbox sharing and accessing your full mailbox from multiple devices at once. If users want to be able to share a mailbox or access their email from their mobile phone then we strongly recommend that you use *VPOP3 Enterprise*.

VPOP3 Enterprise also supports multiple calendars using the CalDAV standard and other 'enterprise' features such as using an external database for distribution list membership and address books. *VPOP3 Enterprise* also supports [SSL/TLS](#) connections to its own services as well as [SSL/TLS](#) connections to remote servers.

VPOP3 Basic

VPOP3 Basic is a reduced-functionality version of *VPOP3*. It does not support [IMAP4](#) for email, just [POP3](#), which does not allow shared access to mailboxes or access to your full mailbox from multiple devices. *VPOP3 Basic* supports the CalDAV standard, but each user can only have a single calendar.

VPOP3 Basic supports [SSL/TLS](#) connections to remote servers, but does not support installing a certificate for [SSL/TLS](#) connections to its own services.

VPOP3 Home User

VPOP3 Home User is a cut-down version of *VPOP3 Basic*. It only supports 5 users (and cannot be upgraded above that). Some other functionality such as [LAN Forwarding](#) is also disabled. We don't recommend that the Home User version is used by businesses.

3.3 Administrators

In *VPOP3*, an **Administrator** is a [User](#) who is [defined as an administrator](#). You must have at least one **Administrator**, but there is no limit to how many you can have - if you wish, *all* your **Users** could be **Administrators** (but this is not recommended!)

In *VPOP3*, there is only one level of **Administrator**, so a **User** who is set as an administrator can access all the settings, mailboxes, etc.

For an **Administrator** to log into the [VPOP3 Settings](#), they use the same username & password as they would use to access their Webmail pages. This is usually the same username & password which they would use to collect & send mail, but it is possible to [have a different Webmail password](#) if you wish.

Default Administrator account

When you install VPOP3 for the first time, it will create an initial **Administrator** account for you. You can set the details for this account to be whatever you wish, but the defaults are:

- Username: *postmaster*
- Password: *admin*

There is nothing special about this initial administrator account. Generally, we recommend that a normal **User** account is used as the administrator account. That uses one fewer licensed user, and means that system error messages (which are sent to the [Main Administrator](#)) are less likely to be missed.

Deleting an Administrator account

Because VPOP3 requires at least one **Administrator** account, it prevents you from deleting the account you are currently logged in as.

So, to delete an **Administrator** account, you need to log in as a different **Administrator** user, and then delete the account you want deleted.

For instance, if you installed VPOP3 using the default *postmaster* administrator account, and now want to remove that user, and use your own account as the administration account instead, you should:

1. Set your own account to be an **Administrator**
2. Log out of the *postmaster* account
3. Log back into the [VPOP3 Settings](#) using your own account details
4. [Delete](#) the *postmaster* user

3.4 Email protocols

Email protocols are defined by a set of standards which allow email software on different platforms and from different vendors to communicate between each other. VPOP3 supports all the major email protocol standards (IMAP4 is only supported in [VPOP3 Enterprise](#)).

- [POP3](#) - basic email protocol to allow downloading mail from an email server to a client
- [SMTP](#) - email protocol for sending mail from an email client to a server or between email servers.
- [IMAP4](#) - feature-rich email protocol to allow storing of mail on an email server with the client synchronising with the server
- **Webmail** - to access email via a web browser (not really an email protocol)
- [SSL/TLS](#) - a layer on top of POP3/SMTP/IMAP4 to support server verification and encryption of email protocol sessions.

3.4.1 POP3

The base POP3 protocol is defined in [RFC 1939](#).

POP3 is a simple protocol where mail arrives in a POP3 server (usually at your ISP or on a local server such as VPOP3). The email messages are put into a mailbox on the server. Then, an email client (eg

Windows Live Mail, Mozilla Thunderbird or a mobile phone etc) will log into the POP3 server and retrieve messages from the server, and (usually) delete them afterwards and then log off. The main place where messages are stored when using POP3 is on the email client, so you should ensure that it is backed up regularly.

The POP3 protocol usually uses port 110, but an old method of [encrypting traffic](#) often uses port 995 instead.

POP3 is very basic and does not have any facilities for folders, or even marking messages as 'read'.

If the email client is configured to leave messages on the server, then the client has to keep track of which messages it has already downloaded. It does this using a command called 'UIDL' (Unique ID List) which retrieves a list of unique message IDs assigned to the messages by the POP3 server. This is not foolproof because sometimes the server may reassign unique IDs, or reuse a unique ID causing duplicated messages or missing messages, but these problems are quite rare with well designed POP3 server software.

If the email client is configured to NEVER delete messages, then it will get very slow after some time because every time the email clients logs on it will need to retrieve a full list of the unique IDs, then it will have to compare that list to its own list of which messages have already been downloaded, and then download the messages. There is no requirement for the POP3 server to store messages in order of receipt, so it is impossible to shortcut this process.

POP3 is designed so that only one email client can log into a specific mailbox at once. If a second client attempts to log on at the same time, it should be refused access. If two clients could connect at once, and one client deletes a message, there is no mechanism to inform the second client that the message has been deleted, so it may be unable to download the deleted message which will probably confuse the POP3 email client because that is something that should never happen according to the standards.

When messages are deleted by the email client they are not deleted immediately. Instead they are deleted when the email client logs off with a QUIT command. This helps to prevent messages being lost if the email client crashes. However, it can cause confusion because you may see messages being deleted but they don't actually get deleted.

If new messages arrive in a POP3 mailbox, they will not be visible to the email client until it logs off and back on again. This is why POP3 clients are designed to 'poll' for messages, and email clients may have a 'Send/Receive' button to trigger a poll.

It is possible to have two email clients logging into a single POP3 mailbox, as long as they don't both log in at the same time. If the email clients are configured to leave messages on the server for a couple of days, then they will both get all the messages. However, any message management (eg deleting messages or organising into folders) will have to be performed twice.

[IMAP4](#) was designed to solve many of the limitations of POP3.

A sample POP3 session might go like this:

```
+OK POP3 server ready
USER fred
+OK Enter password
PASS letmein
+OK 5 messages (61241 octets)
STAT
+OK 5 61241
LIST
+OK 5 messages (61241 octets)
1 1241
2 23451
3 3321
```

```
4 5667
5 27561
.
UIDL
+OK 5 messages (61241 octets)
1 anh-637722
2 anh-637723
3 anh-637727
4 anh-637729
5 anh-637735
.
RETR 1
+OK 1241 octets
<message content>
.
DELE 1
+OK message 1 deleted
QUIT
+OK signing off
```

3.4.2 SMTP

The base SMTP protocol is defined in [RFC 5321](#).

SMTP is the Internet protocol which is used on the internet for sending email from one computer to another. It is widely known as the protocol used when individuals send messages from their email client (or MUA - Mail User Agent) to their own (or their ISP's) mail server (or MSA - Mail Submission Agent), but it is also used for mail servers (or MTAs - Mail Transfer Agents) to send messages between each other.

SMTP is a relay protocol; messages are passed along a chain of mail servers like a baton in a relay race. Once the receiving server has acknowledged receipt of the message, the sending software has to assume it will be delivered or a delivery status notification message will be returned to the sender. The sending software has no way of finding out what happened to the message once it was acknowledged by the receiving server.

Types of SMTP

There are two 'types' of SMTP server, but they are very closely related and use mostly the same commands so the roles can be combined. An MTA is used for sending mail from one server to another. This MUST use TCP port 25 for transmission and can support negotiated 'STARTTLS' encryption. An MSA is used for a user to send mail to (and will typically then send the message to an MTA). These usually use TCP ports 25 or 587, they may occasionally use port 465 if they use an old method for [encrypting traffic](#). An MSA should require SMTP authentication and encryption, an MTA must not *require* authentication (or other servers won't be able to send mail to it because they won't know any authentication details) and must not *require* encryption (to allow receiving messages from older MTAs which may not support encryption). It is possible for software to listen only on port 25 and behave like an MSA if authentication is used or an MTA if it isn't.

SMTP authentication

SMTP authentication is optional in the protocol. Most well configured SMTP servers will require some form of authentication to be able to send outgoing mail (otherwise the server is in a state known as 'open relay' which is *BAD THING*), but MTAs will not require authentication for incoming mail to local recipients.

There are three forms of authentication used in SMTP:

- The oldest is authenticating by looking at the sender's IP address. ISPs will often only allow the use of their SMTP servers by customers who are on one of that ISP's IP addresses.
- Then there is 'POP3 then SMTP' authentication. This was often used before 'proper' SMTP authentication was available. In this method the user has to collect mail using POP3 first, then the ISP's server will remember that user's IP address for a few minutes so they can send mail from the same IP address immediately after checking for mail.
- "Proper" SMTP authentication was finally added to the SMTP protocol in 1999 (SMTP itself has been around since 1982). This allows the user to log in using a username & password. Most MSAs and MUAs support this type of authentication nowadays. The login details can be sent in plain text (AUTH PLAIN or AUTH LOGIN) or encrypted using a one-way hash (AUTH CRAM-MD5).

SMTP Data

In an SMTP transaction there are two parts of data:

- The first is the *SMTP Envelope* - like a normal mail envelope, this contains the sender's address ('return path') and the recipient(s) address(es). Normally when the message is delivered into a mailbox (e.g. POP3 or IMAP4) then the SMTP Envelope is discarded so the recipient cannot see it.
- The second part is the *Message Data* - this contains the message content itself (like the letter in a normal mail item). This may or may not contain the sender and recipients, or may even contain different sender and recipient addresses from the envelope, but these addresses are not used for routing messages.

The 'return path' for a message is notionally where it came from. This is actually used as the email address to send bounce (delivery failure) messages to. Note that it is trivial for a sender to forge the return path (or any of the message content) so it cannot be used for authentication. A special case return path is a blank one. This indicates that bounce messages should not be generated. Typically this will be used with automated messages such as bounce messages or autoresponder messages because you do not want to generate bounce messages in response to bounce messages or you can end up with a bounce message loop.

To help with diagnosing problems, an important part of SMTP is that each MTA which the message passes through will add a line beginning with *Received:* to the **top** of the message. This means that you can read the *Received:* headers from the bottom upwards to see the path the message took to reach you (however, note that it is possible for the earlier header lines to be forged by the sender).

A sample SMTP session might go like this:

```
220 mail.example.com ESMTP server ready
EHLO mail.domain.com
250-Hello mail.domain.com, I'm pleased to meet you
250-AUTH PLAIN CRAM-MD5
250-SIZE 10000000
250-STARTTLS
250 HELP
MAIL FROM:<bob@domain.com>
250 OK
RCPT TO:<joe@example.com>
250 OK
RCPT TO:<katy@example.com>
550 Recipient not recognised
RCPT TO:<kate@example.com>
```

```
250 OK
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: test message
From: Bobby Tables <bob@domain.com>
To: joe@example.com,katy@example.com,bill@example.com

This is a test message
.
250 OK - queued as 6234efgge9gwkw6d
QUIT
221 Bye, see you later
```

ETRN and ATRN

SMTP is a 'push' protocol where messages are pushed from the sender to the recipient (unlike POP3 & IMAP4 where the recipient goes and collects the messages). In some situations a push protocol doesn't work well, such as when the recipient has an intermittent Internet connection.

The ETRN (Extended TuRN) and ATRN (Authenticated TuRN) commands were designed to allow SMTP to work in these situations. The mechanism that uses ATRN is also known as [ODMR](#) (On-Demand Mail Relay).

VPOP3 supports both [ETRN](#) and ATRN/ODMR connections. The ISP has to support them as well for them to be used.

With ETRN, the recipient sends an ETRN command to an SMTP server which tells that server (or a related server) to start sending messages for the specified domain to an SMTP server on a known IP address. There is no authentication in this case because the messages are sent to a known IP address linked to the domain. There are two SMTP sessions in this case

ETRN Session 1

Client C1 at the user connects to server S1 at the ISP

```
C1 > ETRN mydomain
```

```
S1 < 250 OK queuing started
```

```
C1 > QUIT
```

```
S1 < 250 Goodbye
```

ETRN Session 2

Client C2 at the ISP connects to server S2 at the user (note the other way around from Session 1) and sends mail using SMTP as for a normal SMTP session.

With ATRN, the recipient logs into the remote SMTP server using SMTP authentication and then sends an ATRN command. Now, the same session switches modes, so the SMTP client becomes the server and the SMTP server becomes the client. This will work with dynamic IP addresses because the session has been authenticated and there is only a single session.

ATRN Session

Client C at the user connects to server S at the ISP

```
C > EHLO client.com
S < 250-myisp.com
S < 250 ATRN
C > AUTH LOGIN <login details>
S < OK
C > ATRN mydomain.com,mydomain.org
S < OK now reversing the connection                - from now on the server acts as the
client and the client acts as the server
C > 220 client.com ready to receive mail
S < EHLO myisp.com
C > 250 client.com
S < MAIL FROM:<...>
etc - standard SMTP session now, but with 'S' sending the commands and 'C' responding
```

3.4.3 IMAP4

The base IMAP4 protocol is defined in [RFC 3501](#).

IMAP4 was designed to solve many of the limitations of [POP3](#). With IMAP4, mail arrives in an IMAP4 server (usually at your ISP or on a local server such as VPOP3). The email messages are put into an Inbox folder in a mailbox on the server. Then, an email client (eg Windows Live Mail, Mozilla Thunderbird or a mobile phone etc) will log into the IMAP4 server and synchronise with the server. The main place where messages are stored when using POP3 is on the email server, so you should ensure that it is backed up regularly. Usually the email client will keep a cached copy of the mailbox on the user's computer to improve performance, but it will resynchronise down from the server whenever it connects (this means that if messages disappear from the server, the client will delete them from its local cache when it connects to the server, it will *not* upload them back to the server).

Because the mail is stored on the IMAP4 server, this means that it has features for managing folders, copying messages between folders, searching for messages, marking messages as read/answered etc.

Unlike POP3, with IMAP4, actions take effect immediately. If the IMAP4 client deletes a message, the message is deleted immediately, and if a new message arrives, it will be visible to the email client immediately. The mail server will notify the email client if new messages arrive, message flags are changed, messages are deleted etc, so the email client can keep its displayed message list and cached copy in synchronisation with the server. This means that usually IMAP4 clients will connect to the server and stay connected. There is no need for them to 'poll' for new messages as with POP3, so usually a 'send/receive' button is redundant.

Multiple email clients can log into the same mailbox at the same time; in fact most email clients will make several simultaneous connections to the POP3 server to perform several tasks at once. The notifications from the server go to all relevant connections, so if 3 email clients are logged into the same mailbox and folder, and a message in that folder gets deleted by one of the clients, all three email clients will be notified of the message's deletion.

Another feature of IMAP4 allows email clients to store messages directly into message folders. This is most commonly used for 'Sent Items' or 'Drafts' folders. The email client will store a copy of sent

messages into a 'Sent Items' folder (this is not the server's responsibility). This means that sent items and draft messages will be available from any IMAP4 client, not just the one from which the message was sent or created.

One feature of IMAP4 which sometimes causes confusion is that message folders can be 'subscribed' to. Most email clients will not display folders which are not subscribed to. This allows you to 'hide' folders you don't want to see any more, however it can cause confusion because folders may seem to disappear if they are unsubscribed from, or folders which have been deleted may still be visible in a folder list, but not accessible, because the folder hasn't been unsubscribed from and email clients will often show subscribed folders whether or not they exist. Usually the email client will automatically subscribe to a folder when it creates the folder and unsubscribe when it deletes the folder so you won't know it is happening, but this is part of the email client behaviour, not the server's, so if the client doesn't manage the subscriptions properly, it can cause apparently strange behaviour.

3.4.4 SSL/TLS

SSL & TLS are encryption methods. They are not used for 'end-to-end' encryption but for 'session encryption'. Session encryption protects data from being spied on while it is being transferred between the client and server software. It does NOT encrypt the data stored on the server or client. So, for instance, when sending a message using SMTP with TLS, the SMTP session is encrypted so any login details are encrypted and the message details are encrypted, so no one can spy on them in transit. However, the SMTP server will have access to the unencrypted message, so it could be spied on there. If that server is out of your and the recipient's control then you should not send any top secret information using that method.

If you want to send a message so that no one can read it other than the recipient, then you should use an end-to-end encryption method such as [PGP](#) or [S/MIME](#). VPOP3 does not handle encryption or decryption using these methods, but encrypted emails can be sent through VPOP3 without any problems. You can get plugins for many common email clients to support PGP and S/MIME encryption and decryption, but helping with them is outside our remit.

SSL and TLS are very complex systems and we won't go into the technical details here. Basically SSL and TLS are similar systems and the terms are often used interchangeably. In fact SSL was the first system and then TLS replaced it, with TLS 1.0 being based on SSL 3.0. Many systems which support SSL will support TLS and vice versa. With session encryption the two ends of the connection will usually negotiate the type of encryption to use between themselves, choosing the most secure method which both ends support. VPOP3 currently supports all versions of SSL and TLS 1.0, 1.1 and 1.2, however it is possible that software which connects to VPOP3 may not support the later TLS versions. It is recommended to disable SSL v2 and SSL v3 if it does not cause interoperability issues with other software. (As well as the different versions of SSL/TLS there are also various ciphers, such as RSA, EECDF etc, some of which are more secure than others)

In standard Internet protocols which support encryption there are often two ways the encryption can be used.

The 'old' way is to use an alternate TCP port. For instance, HTTP uses port 80 and HTTPS uses port 443. With this system the client needs to know in advance whether encryption is to be used, it connects on the alternate port and the data is encrypted from the start of the connection.

The newer way is to use "opportunistic encryption" (also known as negotiated encryption or STARTTLS/STLS). With this method the client connects on the standard port and then asks the server if

it supports encryption. If the server and client both support encryption, the client can choose to switch the encryption on so that the remainder of the connection is encrypted. This requires less configuration at both ends of the connection, but a 'man-in-the-middle' attack can cause the client not to use encryption (by altering the server responses to indicate that encryption is not possible). To get around this problem it is often possible to tell the client or server that encryption is *required* so it will fail the connection if an encrypted connection is not established.

Encryption in VPOP3

In VPOP3 Enterprise, the general service SSL settings are configured in [Services -> General -> SSL](#) and, where appropriate, individual services can be configured to support optional or mandatory STARTTLS connections (on the standard port) or to use the alternate port (SSL) method of encryption.

In each VPOP3 [Mail Collector](#) or [Sender](#), you can indicate whether to use SSL or required or optional STARTTLS encryption.

3.5 Global Address Book

VPOP3 supports a Global Address Book. This allows users to access a centralised directory of contacts, for details such as their email addresses.

Email clients can read the Address Book using an Internet protocol called LDAP (Lightweight Directory Access Protocol). LDAP has some serious flaws when it comes to updating/writing directory entries, so neither email clients nor VPOP3 supports that facility using LDAP. LDAP was designed for huge centralised address books which would be managed from a central location, not as a shared contact system which would be updated by many different users, possibly simultaneously, but LDAP is the most widely supported protocol in email clients.

Users can also access the VPOP3 Address Book using their Webmail facility.

Using LDAP

Email clients usually support LDAP, but they can support it in various ways so not all email clients may use it in all the possible ways:

- The most basic email clients will only allow manual searches for addresses.
- Some will allow scrolling through the entire address book list using some LDAP paging/sorting extensions which VPOP3 supports.
- Some will perform address completion when typing in the To/Cc address fields of an email.

Advanced Users only...

LDAP is a hierarchical database system which may cause some confusion for people not used to it. In most LDAP client implementations, there is a setting called 'Base DN'. This tells it the 'root' of the hierarchical tree that searches will occur from. With VPOP3 this can be set to either <blank> or 'O=VPOP3' to include the whole LDAP database (the most common usage), but can be specified differently to reduce the scope of LDAP searches. For instance, 'OU=External,O=VPOP3' will tell the email client to just search in the externally added address book entries, not the ones automatically added by VPOP3 for local users.

The basic hierarchical tree is shown below. Note that when entering a Base DN you specify the parts in reverse order - eg 'OU=USERS,OU=Internal,O=VPOP3' rather than 'O=VPOP3,OU=Internal,OU=Users'

```

O=VPOP3 -- OU=Internal -- OU=USERS -- UID=<username> (internal user)
  |
  | -- OU=LISTS -- UID=<listname> (internal list)
  |
  | -- OU= External -- OU=VPOP3 -- owner=0 -- UID=<id number> ('global
address book' entry)
    |
    | -- owner=<owner user ID> -- UID=<id
number> (user's personal address book entry)
      |
      | -- cat=<extra
directory ID> -- UID=<id number> (VPOP3 Enterprise only - user's secondary
personal address book entry)
        |
        -- OU=ODBC (VPOP3 Enterprise only - ODBC address
book)

```

In VPOP3 Enterprise, users can create multiple directories themselves which can be shared with other users. These appear as the cat=x,owner=y,OU=VPOP3,OU=External,O=VPOP3 entries above. This means that the LDAP client configuration can be configured to just look in these places.

3.6 Groups

To get to this page, go to Settings → Groups

Name	Enabled	User Count	Force	In Everyone List	Allow Sending Internet Mail	Allow Receiving Internet Mail	Monitor	Admin	Max Outgoing Size (kB)	Reply Address
office	<input checked="" type="checkbox"/>	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0	
sasdadadsda	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	email@domain

If this is checked, all users in this group are forced to have the group's configuration. If this is not checked, new users in this group are given the group's configuration, but the users can then be changed individually

VPOP3 Enterprise 6.20 - Imail.pscs.co.uk - 192.168.66.23 | Idle | In: 44812 | Out: 1

In VPOP3, a Group is a sort of **List** which is also used for assigning permissions and settings. It can be used as a basic distribution list, but that use is secondary. If you are simply wanting a 'distribution group', then in VPOP3 add the users to a [Distribution List](#) instead of adding them to a group. Note that groups cannot be emailed to from externally: They are only accessible by local users.

A user can be a member of a **Primary Group**. This group allows you to override user settings by group if you wish. The Primary Group has settings such as permissions which can override individual user's settings. This means that you can change the settings for a group of users in one action rather than individually. However, note that the User [Bulk Edit](#) option may achieve a similar result and be easier to understand in many cases. A user can only be in one **Primary Group**.

A user can be a member of multiple **Secondary Groups**. **Secondary Groups** do not allow you to override user settings but are used for permissions for IMAP4 folder sharing (and may be used for other permissions in the future).

To create a new Group, press the **New** button. To delete a group press the **Delete** button. To edit a group you edit the entries in the table directly. You do not need to 'Submit' any changes on this page, they occur immediately.

If you hover over a cell in the table, the text at the bottom of the screen will give you information about that setting.

Some of the controls are three-state checkboxes. In these cases, if the checkbox is checked as normal, then all members in the group will be made to have this setting set; if the checkbox is clear, then all members will be made to have this setting unset, and if the checkbox is greyed, then all members in the group can have their own individual setting (that particular setting is not affected by the group configuration).

- **Name** - this is the Group name. It cannot be the same as any user or list. When the group is used as a distribution, this is the part of the email address to use before the @ symbol.

- **Enabled** - if this is checked, the group's users are enabled. If it is not checked, then the users are disabled and will not be able to access VPOP3. We have seen this feature used in a school environment where pupils' accounts are in groups by form, and the forms who are meant to be using computers are enabled as appropriate.
- **User Count** - this is a count of how many users are in this group (readonly).
- **Force** - if this is checked, then all users in the group will have the assigned settings, and they cannot be changed individually. If this is not checked, then new users in this group will have the group's settings, but they may then be changed individually.

The remaining options in the table relate to user settings which can be configured by group options. Click on the option name to see it in the user's settings.

- [In Everyone List](#) - if this option is checked, then group members will be put into the "Everyone" list.
- [Allow Sending Internet Mail](#) - if this option is checked, then group members can send outgoing email. If it's not checked, then they will be blocked from sending outgoing mail (note that requiring SMTP authentication is recommended if you want to enforce sending limits).
- [Allow Receiving Internet Mail](#) - if this option is checked, then group members can receive incoming email. If it's not checked, then incoming email to them will be treated as if the recipient was unrecognised.
- [Monitor](#) - if this option is checked, then messages to members of this group will be [Monitored](#).
- [Admin](#) - if this option is checked, then the group's members will be administrators.
- [Max Outgoing Size](#) - if this option is set to 0 (zero), then there is no group limit on the size of messages, but if it is set to a non-zero value, then that is the maximum outgoing message size that the group members can send (in kB). This does not limit internal messages, just outgoing ones.
- **Reply Address** - this option lets you set an "Change outgoing mail sender address" option for a whole group of users at once. If you specify a normal email address, then that email address will be used for all members of the group, but if you use an address starting with a *, such as *@mydomain.com, then the * will be replaced with the username of the user

3.7 ISP

An ISP is an Internet Service Provider. This is someone who provides you with an Internet service, such as being able to connect to the Internet using a broadband, leased line, satellite or dial-up connection.

ISP is a broad term so often includes MSPs (Managed Service Providers) and ESPs (Email Service Providers) as well as Internet domain hosting and web hosting companies etc. In this manual we generally use ISP to cover all these cases.

In many situations the connectivity provider also provides email services and web hosting so is the same company, but you may use one company for your Internet connection and a different company for your Internet domain registration and hosting and yet another company for your email services. There is no need at all for them to be related.

3.8 LAN Forwarding

LAN Forwarding is the term we use for sending mail from your VPOP3 mail server directly to other SMTP servers. It is called 'LAN Forwarding' because it is usually performed on a local network, but it can often be used across the Internet as well.

LAN Forwarding is different from normal outgoing mail because:

- you have to tell VPOP3 which mail server to send the messages to. It cannot use DNS MX record lookups to find the appropriate server
- VPOP3 assumes the remote server is always available. [Connection scheduling](#) is not used with LAN forwarding.
- the LAN Forwarding queue is separate from the normal outgoing message queue.

LAN forwarding is mainly configured in the [Settings](#) → [Local Mail](#) → [LAN Forwarding](#) → [Configuration](#) page and you can monitor the LAN Forwarding queue in the **Queue Status** page.

You can also set up LAN forwarding in most places where you can specify a target email address, such as in distribution lists or user forwards/assistants. To do this specify the target email address as:

```
"SMTP:<email address>@[<user>":"<pass>"]<server>":"[<port>]"
```

<user>:<pass>@ and :<port> are optional

So, a simple target would be:

```
SMTP:bob@example.com@192.168.1.1
```

This will tell VPOP3 to send the messages to bob@example.com on the SMTP server at 192.168.1.1, not using authentication and on the standard SMTP port 25

A more complex target would be:

```
SMTP:bob@example.com@fred:mypass@192.168.1.1:587
```

This will tell VPOP3 to send the messages to bob@example.com on the SMTP server at 192.168.1.1, logging on using the username 'fred' and the password 'mypass', and sending on the SMTP submission port 587

3.9 Lists

In VPOP3 a **List** is a way of sending email to a group of email addresses. There are two types of List in VPOP3:

- [Distribution Lists](#) - simple way of distributing mail to a group of email addresses with no options.
- [Mailing Lists](#) - more flexible way of distributing mail to a group of email addresses with many options.

There are also [Groups](#) which are slightly different in that they can only contain local users and aren't as configurable.

Lists can contain local email addresses and remote email addresses. You can also include lists inside other lists, and they will be expanded as necessary.

To send messages to a List, you simply send a message to the <listname>@<local domain>, so if your domain is *example.com* and the list is called *distributors*, then to send a message to the list members you would send it to *distributors@example.com*.

3.9.1 Distribution Lists

In VPOP3 a Distribution List is a simple list of email addresses which can have messages sent to it by emailing one address. For instance, if you have a list called *customers*, then you could email all your customers by sending a message to *customers@mycompany.com*. VPOP3 will BCC all the list members and distribute the message to both local list members and remote list members as appropriate.

A Distribution List is the simplest type of list in VPOP3, there are no other options for the list other than the list of members.

Also, see the [configuring a distribution list](#) topic.

A couple of possible problems with a Distribution List are:

- Because the message is delivered to the list members immediately, if large messages are sent to a distribution list containing a large number of local recipients, it may take some time for the message to be distributed to all the local users, especially if the server is a bit slow. In some cases the sending email software may timeout while the message is being distributed if the timeout is set too short. This can occasionally cause the sending email software to silently retry the message so that the recipients may receive multiple copies. Increasing the send timeout in the email client or using a [Mailing List](#) instead will solve this problem.
- Because the message is BCCd to the recipients, this can cause delivery problems if any of the remote recipients are using a shared POP3 mailbox for their mail, or if they have filters designed to block BCC messages. Using a Mailing List with the [Slow Message Posting](#) option will solve this problem because VPOP3 will send a copy to each recipient with their email address in the To header field.

3.9.2 Mailing Lists

In VPOP3 a Mailing List is a list of email addresses which can have messages sent to it by emailing one address. For instance, if you have a list called *customers*, then you could email all your customers by sending a message to *customers@mycompany.com*.

A Mailing List is more flexible than a Distribution List. It can do everything a Distribution List can do, and a lot more, but is a bit more complex to configure because of the extra options.

Also, see the [configuring a mailing list](#) topic.

Some of the possible ways you can use a Mailing List are:

- As a simple distribution list - do not allow subscriptions or moderation, allow anyone to post to it, don't perform any header modifications, etc
- As an announcement list - only allow moderators to post to it, modify the header so that replies come back to an 'enquiries' type email address, allow subscriptions and unsubscriptions.
- As a discussion list - allow members to post to it, modify the header so that replies go back to the list rather than to the original sender, allow subscriptions and unsubscriptions.

3.10 Mail Connectors

VPOP3 has three types of **Mail Connector** which are configured by going to the [Mail Connectors](#) tab in the VPOP3 settings:

- Connections
- Mail Collectors
- Mail Senders

These are summarised below, along with the **Connector Schedule** which is linked tightly with these

Connection

A **Connection** tells VPOP3 how to connect to the Internet. Nowadays, these are usually set to connect via a router, and have very little configuration.

In the past (and still, in some specialised configurations), a **Connection** may tell VPOP3 to connect using a dial-up connection which VPOP3 controls. These have much more configuration involved.

VPOP3 can have up to 10 **Connections** defined

Mail Collectors

A **Mail Collector** tells VPOP3 how to collect mail from a remote mail server (usually your Internet Provider).

Usually this tells VPOP3 how to collect mail from an external [POP3](#) server. It can also be used to tell VPOP3 to trigger an incoming [SMTP](#) feed (e.g. on dial-up connections, or if you need to send an **ETRN** command) or to start an **ODMR** (also known as **ATRN**) mail collection.

You do not usually need to use a **Mail Collector** to have an [incoming SMTP feed](#) with a permanent Internet connection.

VPOP3 can have an unlimited number of **Mail Collectors** defined.

Each **Mail Collector** can be associated with one or more **Connections**. There is no limit to the number of **Mail Collectors** which can be associated with a **Connection**.

Mail Senders

A **Mail Sender** tells VPOP3 how to send mail to a remote mail server (e.g. your ISP's *smarthost*), or using [direct MX routing](#) using [SMTP](#).

Each **Mail Sender** is associated with only one **Connection**. Each **Connection** can only have one **Mail Sender**. This means that VPOP3 can have up to 10 **Mail Senders** defined.

Connector Schedule

The **Connector Schedule** tells VPOP3 when to connect to send/receive emails.

Each **Schedule** item tells VPOP3 when to connect using one or more **Connections**. Because each **Connection** can have multiple **Mail Collectors** associated with it, that means that each **Schedule** item can start multiple **Mail Collectors**.

The way that the **Schedule**, **Connections** and **Collectors** are linked means that it is simple to set up the most common scenarios, but it is still possible to have more complex variations.

For instance:

- You can have one **Connection** defined, with multiple **Collectors** defined to collect from several ISP POP3 mailboxes every few minutes, according to the **Schedule**.
- You may want to collect mail from some ISP mailboxes more frequently than from others. In this case, create two **Connections**, and associate some **Collectors** with the first **Connection**, and the rest of the **Collectors** with the second **Connection**. Then, set up two **Schedule** items, one to trigger the first **Connection** more frequently (e.g. every 5 minutes) and the second **Connection** less frequently (e.g. every 30 minutes).

3.11 Mappings

In VPOP3 a **Mapping** is a way of altering the behaviour of an email address.

By default, if you have configured VPOP3 to handle the domain *mycompany.com* and have a user called *fred*, then emails addressed to *fred@mycompany.com* (and only *fred@mycompany.com*) will be put into *fred's* mailbox.

Sometimes you may want to change this behaviour, and this is where **Mappings** are used.

Examples

For instance, with Mappings you can:

Redirect *fred's* mail to someone else

If you create a **Mapping** of *fred* → *kate*, then any messages addressed to *fred@mycompany.com* will be sent to *kate* instead.

Copy *fred's* mail to someone else

If you create two **Mappings**:

- *fred* → *kate*
- *fred* → *fred*

then any messages addressed to *fred@mycompany.com* will be sent to both *kate* and *fred*.

You can specify as many Mappings for an email address as you wish, and VPOP3 will process all of them. However, if you are going to have lots of Mappings, you may be better using a [Distribution List](#) instead.

Have a *fred* email address at two different domains, going to different people

With the default behaviour, if you have set VPOP3 to handle two domains *mycompany.com* and *anothercompany.com*, then messages to *fred@mycompany.com* and *fred@anothercompany.com* will both go to the user called *fred*. In many cases this is exactly what you want, but if that isn't what you want, then you can use **Mappings**.

For instance, instead of creating a [User](#) called *fred*, create two **Users** called *fred.mycompany* and *fred.anothercompany*. Then, create two Mappings:

- *fred@mycompany.com* → *fred.mycompany*
- *fred@anothercompany.com* → *fred.anothercompany*

Make an alias for *fred*

If *fred* is your salesman, then you may want him to also receive messages addressed to *sales@mycompany.com*. In this case, simply create a **Mapping** of *sales* → *fred*.

You could also create a Mapping of *someone@somewhere-else.com* → *fred* and VPOP3 will send messages addressed to *someone@somewhere-else.com* to *fred's* mailbox.

Tell VPOP3 that an email address on your domain exists, but not locally

If your [Local Domains](#) are set to *mycompany.com*, then whenever a message addressed to a user *@mycompany.com*, VPOP3 will assume that the recipient should be defined in VPOP3. This will generate an error if the recipient doesn't actually exist. For instance, if VPOP3 handles most messages for *mycompany.com*, but messages to *kate* are put into a separate mailbox at your Internet provider, you can create a **Mapping** of *kate* → **REMOTE*. This tells VPOP3 that the user *kate* exists, but is not handled by this VPOP3. In this case, locally sent messages to *kate@mycompany.com* will be [sent out to the Internet](#), and VPOP3 will ignore the *kate@mycompany.com* recipient when [downloading messages from a remote POP3 mailbox](#).

Make VPOP3 send messages from a particular address to *fred*

As well as checking the recipient address, **Mappings** can also check the sender's address when downloading from an external POP3 mailbox. This can be useful when trying to get around problems which happen when [using a shared POP3 mailbox with BCCs](#).

So, you could create a **FROM** mapping of *customer@ourclient.org* → *fred* and any messages coming from *customer@ourclient.org* will be sent to *fred*. (Note that [Download Rules](#) also let you do something similar).

Notes

Wildcards

Mappings allow you to specify * and ? wildcards in the address portion of the Mapping. This can be useful in some cases.

Note that we **do not recommend** using a Mapping like *fred@**. While VPOP3 will understand this, it will probably not do what you want. If someone sends a message to you, and CCs it to *fred@a-totally-different-company.com*, then this Mapping would make the local user *fred* receive a copy of the message, which is probably not what you intended.

There is also a 'special wildcard' you can use in Mappings: [~@domain.com](#). In this case, VPOP3 will check this Mapping if the recipient address doesn't match anything else. This lets you create rules for unrecognised addresses.

How Mappings are used by VPOP3

When a message arrives at VPOP3, first of all it looks through the **Mappings** to see if any of those match the recipient address. If they do, then VPOP3 *only* processes the Mappings. If no Mappings

match the address, then VPOP3 will check for matching users/lists using an 'implied Mapping' (unless that option is turned off in the [Mail Collector](#) or [Local Mail](#) settings).

Finally, if no users or lists (or other special addresses) match the recipient address, then VPOP3 will check any ~@... Mappings to see if those match.

3.12 Spamfilter Quarantine

The VPOP3 Spamfilter Quarantine is a place where messages may be placed by the VPOP3 spam filter if they are deemed suspicious enough. The VPOP3 spam filter does not just delete messages because all spam filters have the risk of 'false positives' where legitimate messages are incorrectly detected as spam.

Each VPOP3 user has their own quarantine area where their suspicious messages are stored. Non-user entities (such as lists or forwarding email addresses) do not have a quarantine area so suspicious messages to those cannot be placed into a quarantine for that entity.

VPOP3 will hold the messages in the quarantine for a set time (default 14 days) and then automatically delete them. This time can be configured in the [Quarantine Settings](#).

Every day, VPOP3 will send a message to each user who has at least one message placed into the quarantine. This message will contain a summary of the quarantined messages, along with a link which can be used to view the message (and optionally release it for delivery). It is possible to alter the time when this summary message is generated, and even set VPOP3 to generate more than one a day. Again, this is set in the [Quarantine Settings](#).

Users can access their own quarantined messages at any time by logging into their Webmail account and selecting the 'Quarantine' tab.

Administrators can access the quarantined messages for any user by going to the [Settings -> Spamfilter -> Quarantine Viewer](#) page.

It is possible to disable the quarantine either globally (in [Settings -> Spamfilter -> General -> Quarantine settings](#)) or for an individual user (in [Edit User -> Advanced](#)). In this case, suspicious messages will be delivered to the user instead of placed into the quarantine.

3.13 Users

In VPOP3 a '**User**' is an object which has an associated mailbox and settings. In different software or different situations, a **User** may also be called a **Mailbox** or an **Account**.

VPOP3's licensing is based on **Users**. You purchase a licence for a certain number of **Users**.

You can see how many users you have currently defined by going to the [Users](#) list in the [VPOP3 settings](#). At the top of the page it will tell you how many users you have defined. If you don't have an Unlimited User licence, then it will also tell you the maximum number of users you are allowed to create.

The relationship between VPOP3 **Users** and physical objects is not fixed. In many cases, each VPOP3 **User** may be associated an actual person, but this is not always the case.

For instance, if you have [VPOP3 Enterprise](#), you may have a **User** called *Sales* where all your sales-related email messages go, and then several people may access that mailbox using [IMAP4](#). So, in this case, a VPOP3 **User** may have several people associated with it.

On the other hand, you may have one person who wants to receive mail about different topics and have them kept totally separate - in that case, you may have several VPOP3 **Users** for a single human being.

Email addresses

By default a **User** will have an email address of <*their username*>@<*your domains*>. So, if your email domain is *mycompany.com* and you create a **User** called *kate*, their default email address will be *kate@mycompany.com*. You can change or add email addresses using [aliases](#) or [Mappings](#).

How to decide what Users to create

When deciding what **Users** to create in VPOP3 it can be useful to think how you want mail to be sorted out, and who you want to have access to the different messages.

A common system is to create a **User** for each human who will receive email, then, if you have VPOP3 Enterprise, have an extra **User** for any shared 'department' email addresses - such as *Sales* or *Support*.

Note - if you have [VPOP3 Basic](#), then you cannot have shared mailboxes, so if you want to have several people receive mail for a *Sales* type email address, do not create a separate *Sales* user. Instead, you should use [Mappings](#) to redirect messages for that email address to the relevant **User(s)**.

4 Procedures

4.1 Add SSL Certificate

This topic only applies to [VPOP3 Enterprise](#).

If you want to use session encryption for connections to VPOP3 Enterprise then you need to install an certificate. The certificate should be for the server name used to connect to your VPOP3 server, eg *mail.mycompany.com* or *vpop3.mycompany.com*. You should have a name defined in your domain's DNS records for this server name (an A, AAAA or CNAME record), and your email clients should be configured to use that name when connecting to the server. If you don't do this, then you may get warnings that the certificate name doesn't match the server name. In that case, the connection will still be encrypted, but you lose the benefit of knowing that you are connecting to the correct server (and you aren't subject to a man-in-the-middle attack).

VPOP3 requires the certificates to be in the common PEM format. This is different from the format used by some other Windows software such as IIS etc, but is used for other software including most Linux servers, so it is commonly supported.

Generating and using certificates can be complicated so we recommend either purchasing them directly from us, or from another company which can help with getting them in the correct format for you. If you can get the private key & certificate chain in a suitable format for a web browser such as Apache, then that same private key and certificate chain can be used with VPOP3. Unfortunately, we cannot help with converting private keys & certificates from other formats to PEM format, but there are articles on the Internet explaining how to do this using command-line tools such as OpenSSL.

Basic Steps

The basic mechanism is that you need to generate a CSR (Certificate Signing Request) and Private Key file for your server name using a tool such as OpenSSL or similar. You then submit the CSR to a Certificate Authority such as GeoTrust, Thawte, Comodo or others, and prove your identity to them to show that you are eligible to use that server name (this proof may be as simple as replying to an email to the chosen domain, or as complex as having to send authenticated documents through to them depending on the certificate requirements).

The Certificate Authority will then reply with a signed certificate. You should append the "certificate chain" certificates (supplied by the CA) onto the supplied certificate and install them into VPOP3.

To load the certificate into VPOP3, go to [Services -> General -> SSL Settings](#). Copy & paste the private key PEM file (including the leading -----BEGIN PRIVATE KEY----- and trailing -----END PRIVATE KEY----- lines) into the **SSL Private Key** box and copy & paste the full certificate chain (including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines) into the **SSL Certificate Chain** box, and restart VPOP3.

Using OpenSSL

The instructions below use the command-line OpenSSL tool. You can obtain a pre-compiled version of this toolset from [Shining Light Productions](#).

To generate a CSR and Private Key file, at a command prompt in the OpenSSL\bin directory, run:

```
openssl req -out csr.csr -new -newkey rsa:2048 -nodes -keyout vpop3sslk.pem
```

Enter the details requested by the tool. The most important value is the **Common Name** value which should be the server DNS name - eg *mail.mycompany.com*.

This will create two files: *vpop3sslk.pem* is the file you need to install into the VPOP3 **SSL Private Key** box, *csr.csr* is the file you need to send to the certificate authority for signing.

Once you have the signed certificate back from the certificate authority, open it in Notepad++ or a similar text editor and append the certificate chain files required by your certificate authority (these are different for different CAs, and change from time to time so we cannot tell you exactly what to do here). Then copy & paste all that into the **SSL Certificate Chain** box in VPOP3.

4.2 Allowing remote users access to their VPOP3 mailboxes

Sometimes people want to be able to access their office VPOP3 mail server from a remote site or mobile phone etc.

These instructions assume you have a permanent Internet connection (eg ADSL, Cable etc). If you don't have a permanent Internet connection, see the "[Allow Remote Access to VPOP3 without a permanent connection](#)" topic

Router/Firewall Configuration

First you need to set your router and/or firewall to allow incoming access to the VPOP3 computer on the relevant ports (eg 110 for POP3, 143 for IMAP4, 5108 for WebMail/CalDAV). For details about how to do this you may need to read the documentation for your router/firewall.

If you are using a software firewall, such as the Windows firewall, or other Internet Security software you may need to do the same to allow connections to the VPOP3 software.

With the Windows firewall or Internet security software, you may need to 'allow' VPOP3 to act as a service on the Internet and also allow the specific ports through the software firewall as well.

VPOP3 Configuration

POP3/IMAP4/Webmail

By default VPOP3 will refuse access to anyone connecting from outside your local network, so you need to tell VPOP3 to allow access from anywhere.

Go to Services → POP3 (or Services → IMAP4, or Services → Webmail, as appropriate). Then, go to the [IP Access Restrictions](#) tab. Press the **Add** button. Choose:

- **Allow**
- **Type: Any Host**
- In the **Users** list, either leave all users unselected to allow any user to access the VPOP3 service from the Internet, or select users to just allow those users to access VPOP3 from the Internet.

Edit Access Restriction

Allow
 Block

Type : Any Host

Users : cheryl
 echo
 faxmaster
 fiona
 hannah

Save Cancel

SMTP

Note do NOT simply allow access to anyone to your VPOP3 SMTP service, this will lead to you making VPOP3 into an open relay. Instead you will need to set the SMTP service access restrictions to limit access to your users alone.

Go to the Services → [SMTP](#) page in the VPOP3 settings.

Check the **Require SMTP Authentication** and **Do not require SMTP authentication for internal/incoming mail** options.

Make sure the **SMTP Anti-Relay Protection** method is set to **Check Client IP Address**.

Go to the [IP Access Restrictions](#) tab

The default settings will have **Block - routers** and **Allow - Local Nets** entries. These will block the router itself from sending outgoing email, and anyone on the local network will be able to send outgoing mail.

Now you have checked the **Require SMTP Authentication** box, local users will still be able to send mail, but only if they change their email client configuration to use SMTP authentication. If you wish, you may edit the **Local Nets** entry and check the **Allow Unauthenticated Access** box to allow your local users to send mail without authenticating. If you have added any other 'trusted' networks, eg other subnets on your office network, you may also choose to do the same for those.

Then, add another restriction to **Allow - Any Host**. Do NOT check the **Allow Unauthenticated Access** box for this entry. This lets any user send mail from anywhere as long as they have authenticated first.

If you wish, you can select Users who can send mail from the Internet. If you don't do this, then any user can send mail from the Internet.

Please make sure that passwords for users who can send mail from the Internet are secure. If they are not (for instance if they are 'password' or the user name (or simple variants thereof)) then spammers will often find the login details and send spam through your server.

Email client settings

For the user to access their mail, they connect to the Internet, and use your external Internet IP address assigned by your ISP. Use the same login details as for internal access.

If your office has a static IP address on the Internet, then you can simply use that address as the server address in your email client. If you have your own domain, you can make it easier to remember by configuring a DNS name to refer to that IP address.

See also: [Determining your VPOP3 server address](#).

If you have a static IP address and want computers to be able to work from both inside and outside your network, you MAY be able to use the external IP address in both cases if your router supports NAT loopback, or you may need to set up two DNS servers (or a single DNS server with “zones”). For instance you can create a host name with your ISP for your domain name to resolve to the external IP address for access from outside your network, and have an internal DNS server (such as that which comes with Windows Server, or Simple DNS Plus or similar) to resolve the same host name to the internal IP address.

If your office has a dynamic IP address, then you need to use a 'dynamic DNS' service to give your IP address a name which you can use in your email client.

If you have any problems with DNS entries (either static or dynamic) then we can help you set them up, but as it is not a VPOP3 problem it will be a chargeable incident.

4.2.1 Allow Remote Access to VPOP3 without a permanent connection

Sometimes people want to be able to access their office VPOP3 mail server from a remote site or mobile phone etc.

The [Allow Remote Access to VPOP3](#) topic explains how to configure VPOP3 to support this if you have a permanent Internet connection (cable, ADSL, leased line etc). If you do not have a permanent connection to the Internet, then you will need to configure a dial-in server on the VPOP3 computer or another computer on the same network as VPOP3.

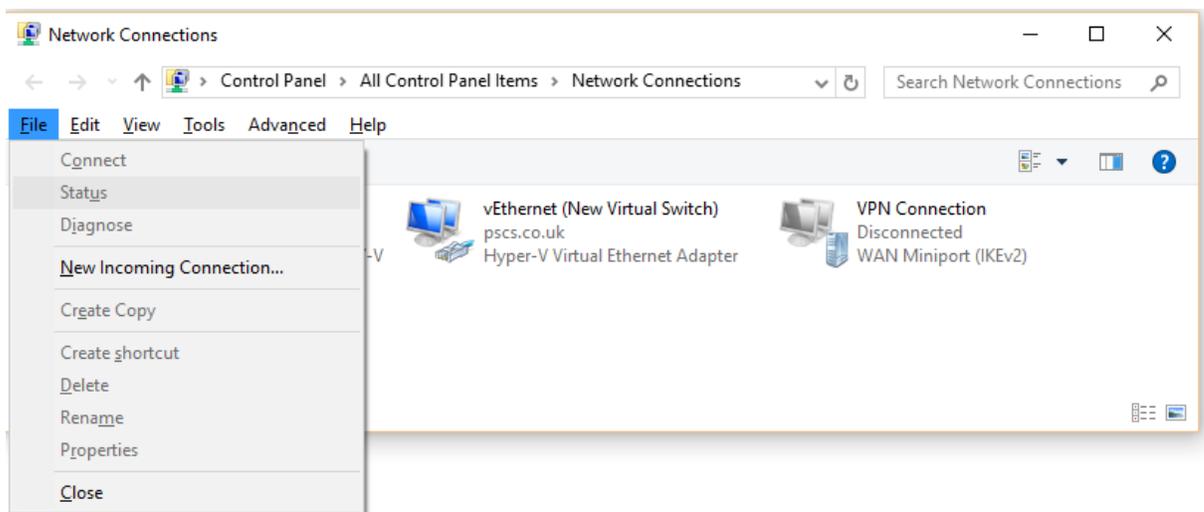
Setting up a dial-in server

To support a dial-in server using these instructions, you need a modem on a Windows computer on the VPOP3 computer or another computer on the same network.

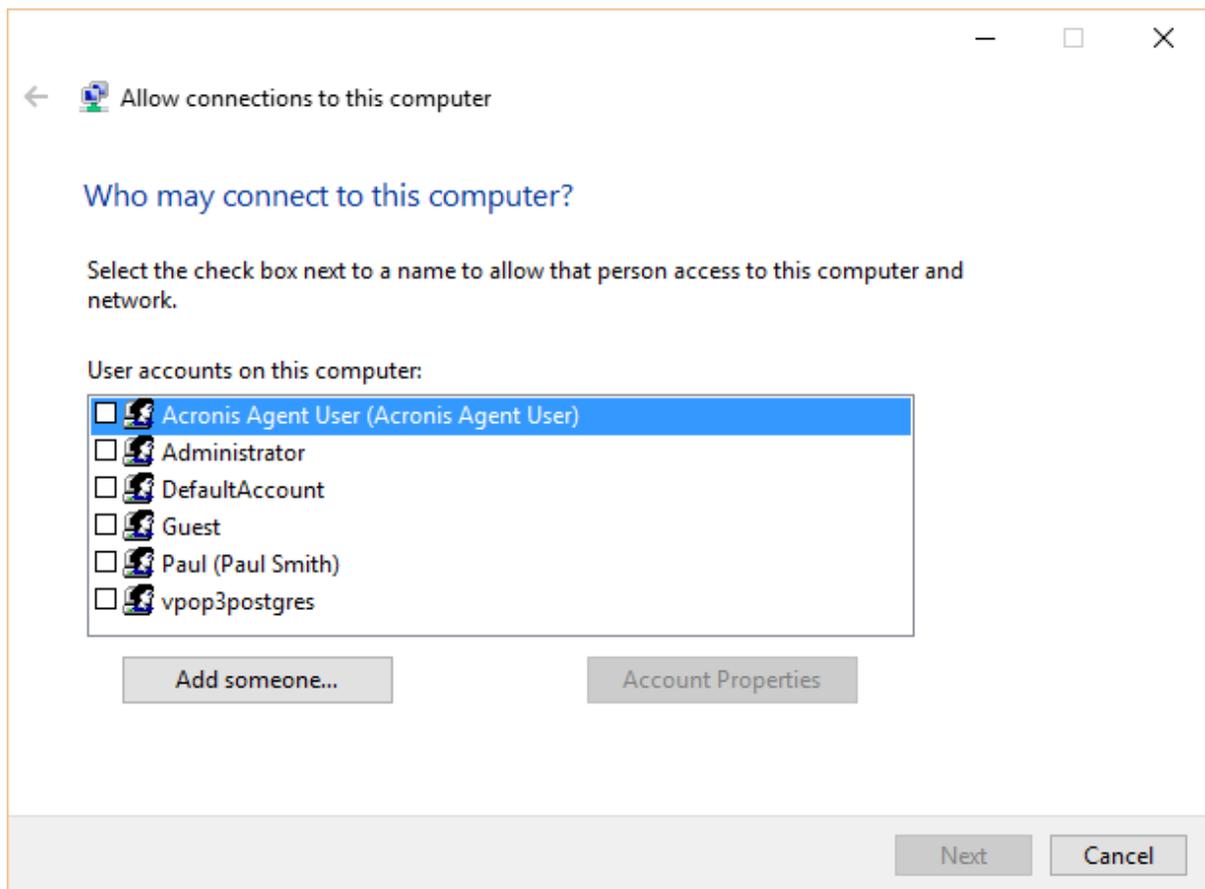
Windows 7, 8, 10

Press `Win+R` to bring up the **Run** dialog. Type `ncpa.cpl` and then OK.

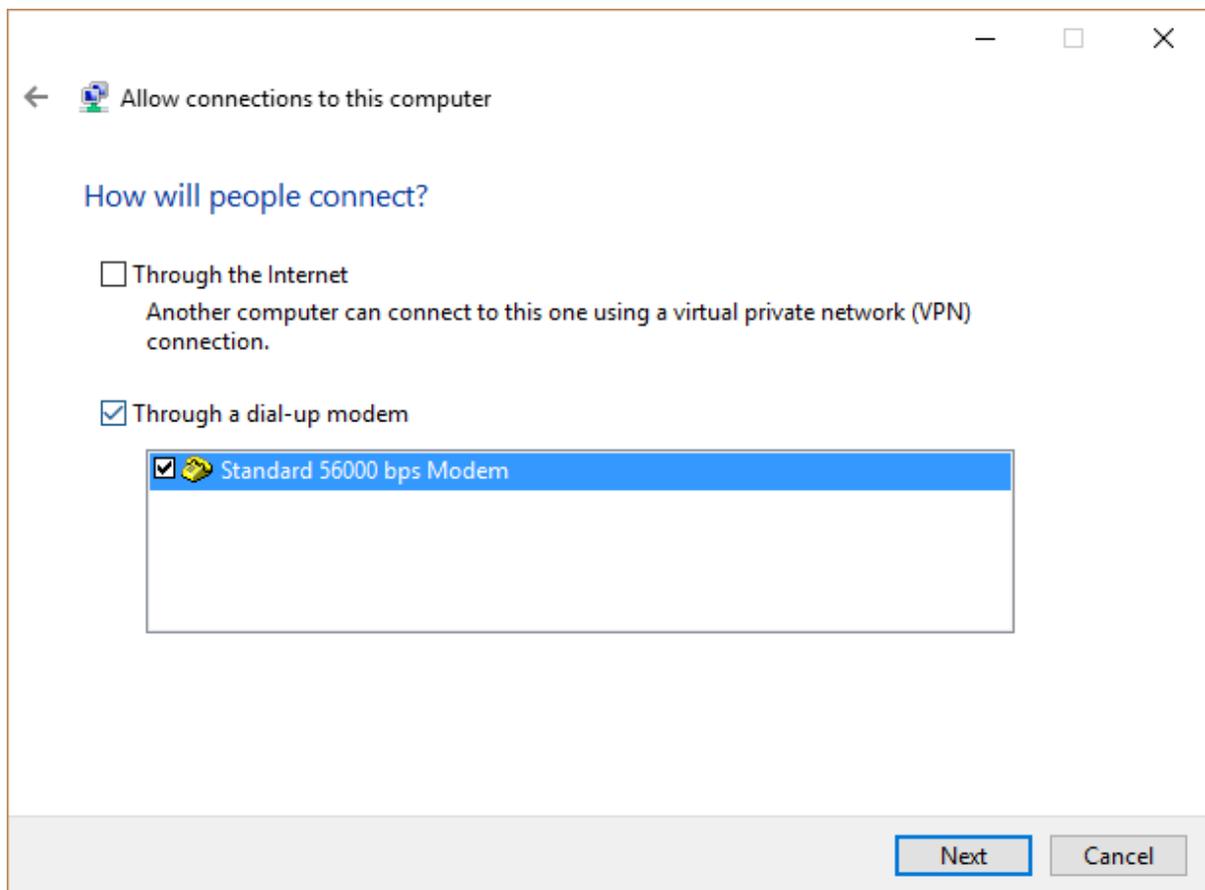
In the window that appears, press `Alt+F` and then choose **New Incoming Connection**



Select the Windows users who you want to be able to dial in to this computer

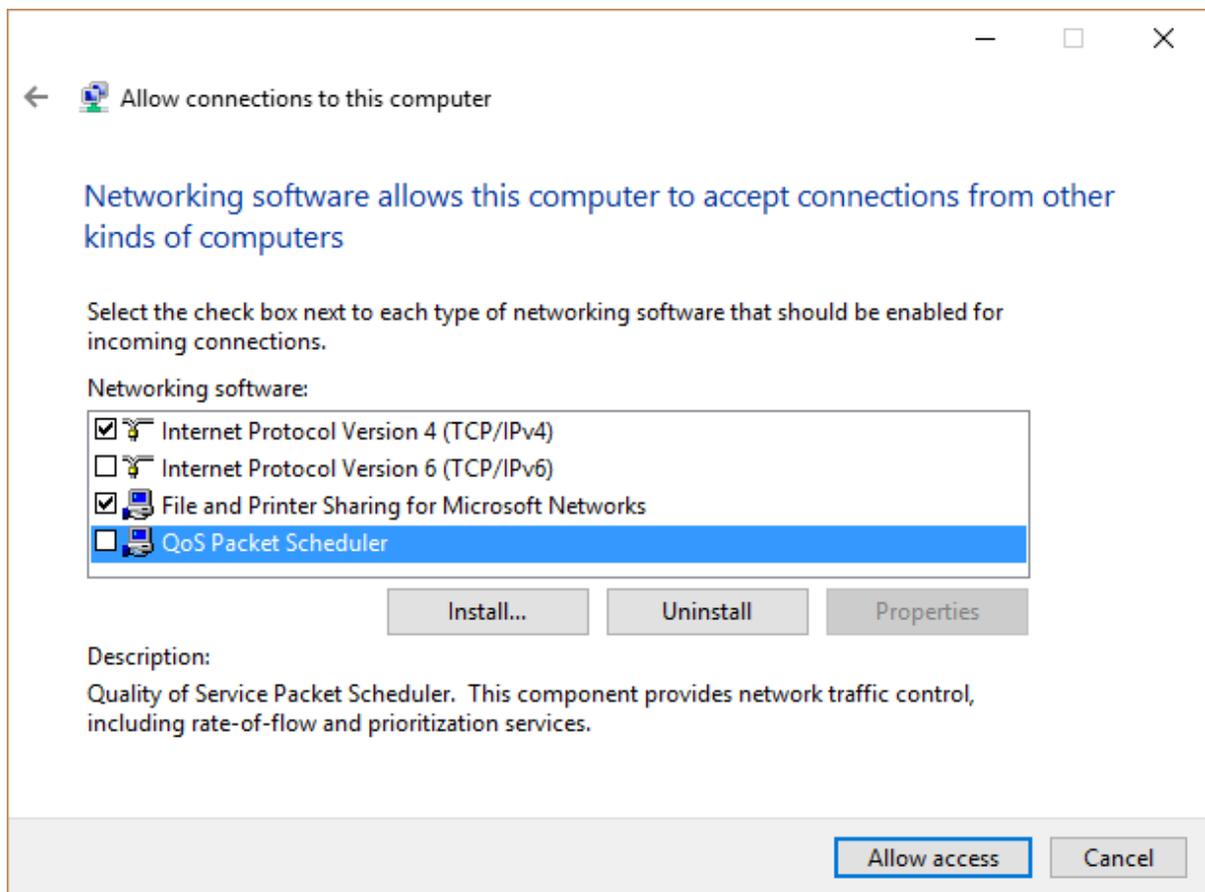


Press **Next**



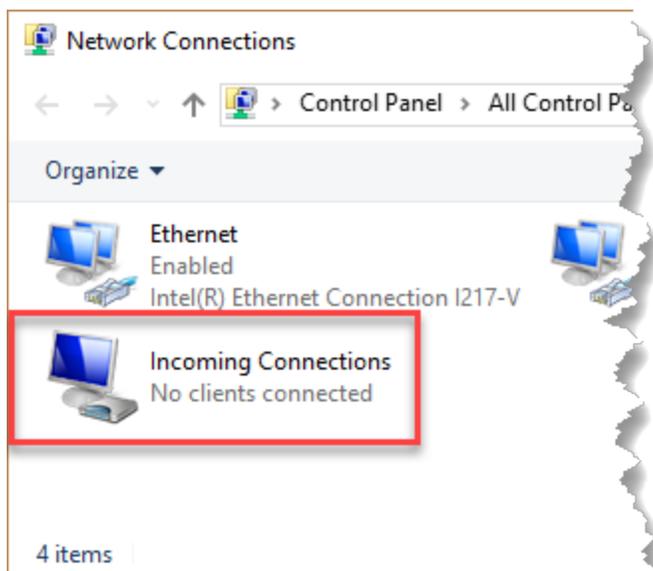
Select **Through a dial-up modem** and select the modem(s) which you want to use for dial-in connections. (If no modem option is available, then Windows does not think there is a modem installed, so go to Control Panel -> Phone & Modems to add one)

Press **Next**



Choose the appropriate network components. VPOP3 only needs TCP/IPv4, but you may want the other services to be available to the dial-in user as well. Press **Allow Access**

Now, in the network control panel there is an Incoming Connections icon which shows how many active incoming connections there are.



VPN

As an aside, at the **How will people connect** dialog, you can also choose **Through the Internet** to have this computer act as a VPN server. This needs a permanent Internet connection so is not relevant for this particular topic, but may be useful in other circumstances - eg if you do have a permanent Internet connection but want to have a VPN for users to connect to VPOP3 rather than connecting simply over the Internet.

Windows Server

Windows Server also supports dial-in services, but it is more complex due to the integration with Active Directory and support for more powerful features.

You need to configure the Windows RRAS (Routing and Remote Access Service) role to support dial-in or VPN connections

For instance see [Windows 2012 - Routing and Remote Access Service](#) for Microsoft's documentation for this service on Windows 2012

4.3 Determining your VPOP3 Server Address

When setting up email clients to connect to VPOP3, you will need to specify a server address (for POP3, SMTP and/or IMAP4). If you don't know what this should be, then these instructions may help. If you are not the technical contact at your company, then you should contact them first, because they may know a 'better' answer.

IP Address

The simplest method to determine the address of the server is to find the server's IP address. Most computers will have two IP addresses, an internal address, and an external address. Use the internal address if you will be accessing VPOP3 across the local network, and the external address if you will be accessing VPOP3 across the Internet.

You need to follow all of these procedures from the computer running the VPOP3 software.

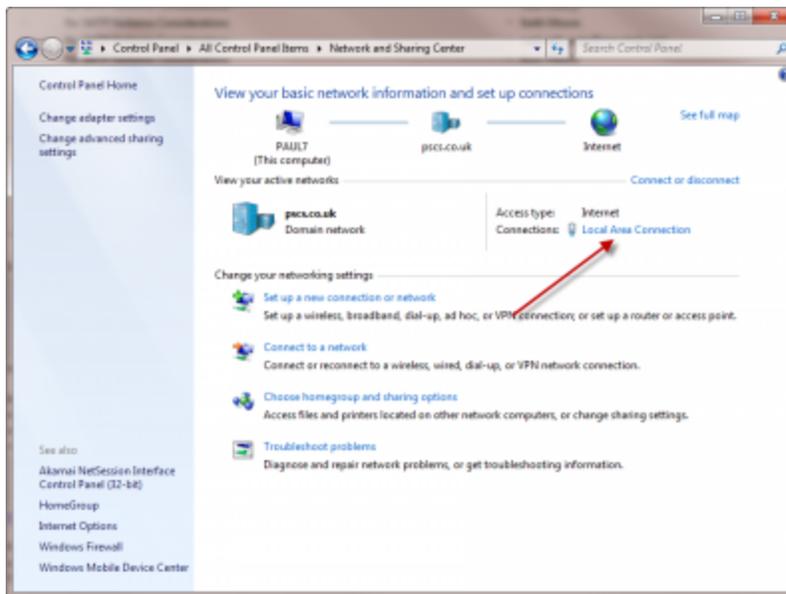
Internal address

There are two main ways of determining this address:

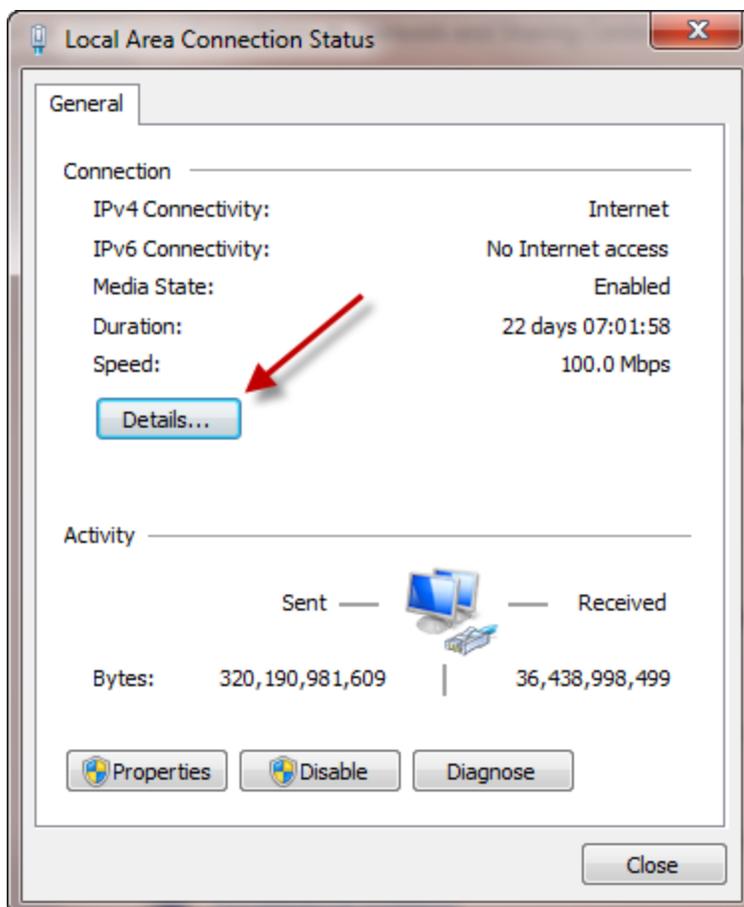
GUI method

This way depends on which version of Windows you are using. These instructions are for Windows 7

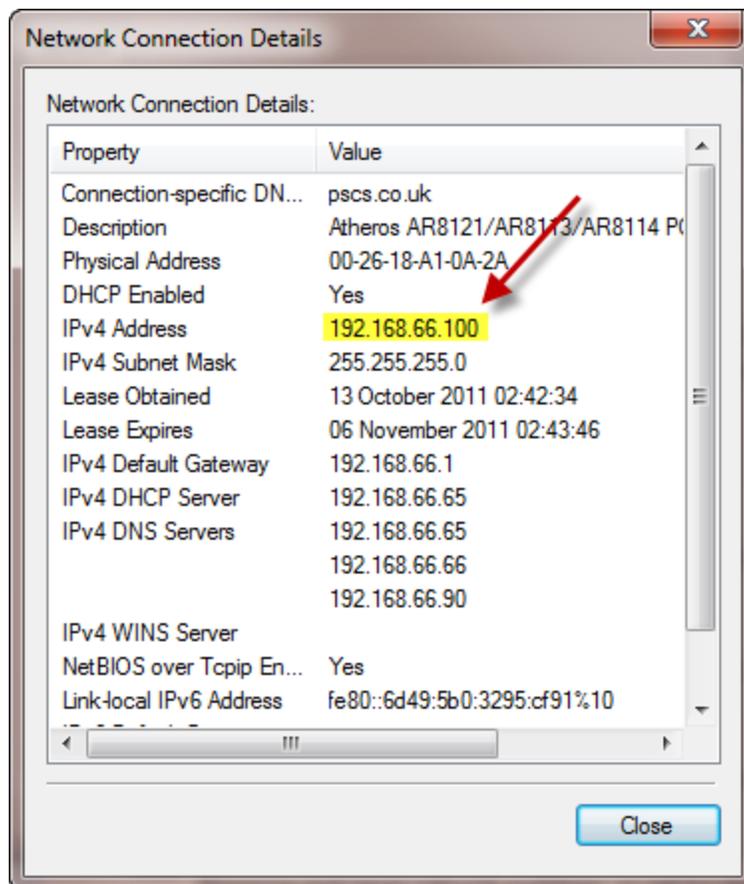
1. Go to **Start** → **Control Panel**
2. Go to either **Network and Internet** → **View Network Status And Tasks** or **Network and Sharing Center**
3. Click on **Local Area Connection** (the exact name may vary, but it is always in the indicated position)



4. You should get a Local Area Connection Status window. Click on Details...



5. In the Network Connection Details window, look at the IPv4 Address value.



That is the IP address of this computer on your network

Command line Method

This way is the same for all versions of Windows.

1. Go to **Start** → **All Programs** → **Accessories** → **Command Prompt** (or **Start** → **Run** → **cmd**)
2. Type **ipconfig** and press Enter
3. In the text that is displayed, you need to look for the line beginning with **IPv4 Address** and use that value.

```

Administrator: Command Prompt

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : pscs.co.uk
    Link-local IPv6 Address . . . . . : fe80::6d49:510:3295:cf91%10
    IPv4 Address. . . . . : 192.168.66.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.66.1

Tunnel adapter isatap.pscs.co.uk:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : pscs.co.uk

Tunnel adapter IP6Tunnel:

    Connection-specific DNS Suffix  . : pscs.co.uk
    IPv6 Address. . . . . : 2001:470:1f08:160d::2
    Link-local IPv6 Address . . . . . : fe80::64f4:6bd1:ecec:2c66%18
    Default Gateway . . . . . : 2001:470:1f08:160d::1

C:\Users\ps.PSCS>

```

You may need to scroll up in the command prompt window if the text has overflowed a single screen.

External Address

If you have a static IP address from your ISP then you can use the external IP address which they have provided you with. If you have a dynamic IP address from your ISP, then this will not work reliably, so you should use the Dynamic DNS method below, or ask your ISP for a static IP address

If you do not know the static IP address which your ISP has provided you with, then you can go to

<http://dns.vpop3dns.com/myip> or <http://www.whatismyip.com>

and these will tell you your external IP address

(there are other similar services)

DNS name

Using a DNS name is easier for users to remember, but it is considerably harder to configure

Internal

To use a DNS name internally, you need to have an internal DNS server, or an external DNS server which can provide an internal IP address

If you have a Windows Server computer, then that will usually have a DNS server Role which you can enable (it is automatically enabled if you use Active Directory)

If you don't have a Windows Server computer, then you could set up a free DNS server such as [ISC Bind](#), or a DNS server such as [SimpleDNS Plus](#)

Configuring your DNS server is beyond the scope of this document. You should consult the documentation for the particular DNS server you wish to use.

Our chargeable technical support service can do it for you if you wish. contact us if you wish to arrange this. The current charge is £30 + VAT per incident.

External

To use a DNS name externally, the method depends on whether you have a static IP address or a dynamic address

Static IP address

If you have a static IP address and your own registered domain name, then simply go to the management console for the registered domain name and add a new Host DNS entry ('A record') with the name being what you wish, eg 'mail' or 'vpop3', and the IP address being your external static IP address. Alternatively, contact your domain hosting company and ask them to make this change for you.

Because there are so many different domain hosting companies, then we cannot give you the specifics of how to do this.

If you have registered your domain through us, then simply contact us and tell us the change you wish to make. There is no charge for this.

Dynamic DNS

If you have a dynamic IP address, then you can set up an account with a company such as dyndns.org (or one of the many other dynamic DNS services), choose a host name and either install the relevant client software on the VPOP3 computer, or configure your router accordingly).

There are so many different dynamic DNS companies, we cannot give you specifics of how to do this, but they usually have instructions you can follow.

Our chargeable technical support service can do this for you if you wish. contact us if you wish to arrange this. The current charge is £30 + VAT per incident.

If you have set up dynamic DNS, and you have your own domain name, you can optionally configure a 'CNAME' record in your domain name configuration to set up an alias of, for instance, 'vpop3.yourname.com' to the dynamic DNS host name. If you do this, make sure that you set the 'TTL' (time to live) to a small number (eg 60 seconds), otherwise there may be a long delay before this alias works correctly if your dynamic IP address changes.

4.4 Incoming SMTP mail feed

Incoming SMTP is how most mail systems on the Internet work. With SMTP, the sender's mail system sends the message to the recipient's mail system, rather than the recipient's system collecting it from the sender.

VPOP3 works fully with incoming SMTP. In fact, on a fresh installation, it will work with incoming SMTP without any setting changes other than telling VPOP3 the [local email domain](#). There are generally other things that you will need to do so that incoming SMTP works correctly, but those are all outside of VPOP3.

Incoming SMTP has two main advantages over other methods such as [POP3 collection](#):

- Messages generally arrive as soon as the sender sends them, rather than at the next "poll time"
- If messages contain BCCs, those will always work with incoming SMTP whereas there can be [problems with BCCs with shared POP3 mailboxes](#).

Requirements

For an incoming SMTP mail feed to work, there are several requirements

- You must have your own email domain (eg 'mycompany.com') and be able to configure DNS records for that domain.
- You must have a static IP address on the Internet. Senders need to know where to send mail to you, so if you have a dynamic IP address they won't know where your mail server is. (You could, theoretically use a dynamic DNS service, but this can be unreliable, and could, in the right circumstances, mean that your mail is delivered to someone else, so it is not recommended!)
- You must have a permanent (or almost permanent) Internet connection. The sender will expect to be able to send you messages as necessary, so if you only connect to the Internet periodically, the chances of the sender trying to send their messages to you at the right times are low. It does not usually matter if your Internet connection may fail occasionally because the sender will usually hold onto messages they couldn't deliver immediately and periodically keep trying to send them over the next couple of days. The exact details of the retries are down to the sender, but this is the usual behaviour. Generally, if your router needs resetting and the Internet is down for a few minutes that won't cause any messages to be lost, but if your Internet connection is down for several days or is only up occasionally then you should not use incoming SMTP.
- You must be able to allow incoming TCP/IP connections on port 25 through your firewall/router, and your ISP must not block these connections.

VPOP3 Settings

These settings are mostly the default settings, so, in most cases, you will not need to make any setting changes.

- In [Settings -> Local Mail -> General](#), you must have the correct **Local Domain** set (alternatively, you can use [Mappings](#) to define all your local email addresses).
- In Services -> SMTP Server -> General:
 - You must have the SMTP service bound to port 25 on an IP address which can be accessed from the Internet
 - You must have **Do not require SMTP authentication for internal/incoming mail** checked
 - You must have **Check Client IP Address** selected in the **SMTP Anti-Relay Protection** method
 - You must have **Reject unrecognised local recipients** checked

DNS Settings

- You must create a DNS 'A' record pointing to the external IP address (usually your static IP address that your ISP provides you with) that your VPOP3 server will be receiving mail on. For instance, this could be *mail.mycompany.com*. The exact name doesn't matter, but it must be in a domain that you control and must not already be in use.
- For the domain(s) where you want messages to be sent, you must create a DNS 'MX' record referring to that domain, and with the MX record set to the name you set in the previous step. The MX priority doesn't generally matter.

The specifics of how you do this will vary from domain hosting company to domain hosting company, so we cannot specify the details here. It's a standard thing to do though, so most domain hosting companies will have instructions on how to do it. For instance:

- [GoDaddy - Add an MX Record](#)
- [Register.com - How do I modify MX records](#)
- [Name.com - Setting up email with MX records](#)

If you have your domain's DNS hosted with us, then you can set it through your domain portal, or just ask us and we'll set it up for you.

Note that, in most cases, we recommend not setting multiple MX records for a single domain. It is generally a bad idea to set your ISP as the "backup MX server" for your domain. Doing this can cause strange problems with spam filtering and other spam reduction systems such as grey-listing, BATV checks etc.

Firewall Settings

You must configure your firewall/router to allow incoming connections on port 25 to your VPOP3 computer. This is usually called "Port forwarding". Again, because there are so many different firewalls & routers, we can't give you details of how to do it, but it is a very common requirement, so your router's documentation should have details. A site which may be useful is <https://portforward.com> which has instructions for many routers and firewalls.

4.5 Restoring a backup

The instructions below are to restore a full backup. You may also be able to [recover deleted messages](#) or [specific message folders](#) if you do not need to restore a full backup.

These instructions are for Version 5 or later. See our [knowledgebase](#) for instructions for earlier versions.

If you just need to restore a database backup into an existing installation of VPOP3, see steps 4 to 7 below.

To restore a full backup of VPOP3:

1. If VPOP3 is already installed, make sure VPOP3 is shut down before starting the restore process
2. If VPOP3 is not already installed or will not run, reinstall VPOP3 into the location where you restored VPOP3. This should reinstall the PostgreSQL database system. Do not start VPOP3 at this time
3. Open a command prompt, and go to the VPOP3 directory
4. If you are restoring the backup over an existing VPOP3 database (especially if the database files are damaged) you will need to DROP the database first. To do this, run:

```
pgsql\bin\dropdb -U postgres -p <port number> vpop3.
```

When it prompts for the password enter the PostgreSQL master password - the default is *pgsql/pass*. (<port number> is usually 5433)
5. Run:

```
pgsql\bin\pg_restore -U postgres -p <port number> -v -C -d postgres <backupfile>
```

where <backupfile> is the backup file you want to restore (usually DBBACK-<number>.DMP). If there are multiple backups available, look at the file timestamps to see which the latest one is. <port number> is usually 5433.
When it prompts for a password enter the PostgreSQL master password - the default is *pgsql/pass*. Note that during this step you may see a couple of errors which are not important: there may be an error about the database already existing, and also an error that the 'plpgsql' language is already installed. (Each of these errors may have several lines in the output). If there are lots of errors, then there may be a problem and you should contact [support](#) for help.
6. Start VPOP3

5 Admin Settings

To access the VPOP3 settings, see the [Getting to the VPOP3 Settings](#) topic.

Notes

In the VPOP3 settings:

- The top of the settings page has sections ([Users](#), [Lists](#), etc) which take you to main areas of the



VPOP3 settings. If the web browser width is too small, then only the icons may be visible, not the accompanying text. In this case, you can hover over the icons to see the text, or expand the browser width to make the text visible.

- This icon: will show some help on the accompanying field if you hover the mouse cursor over it. We have included tips like this for many of the more complex settings in VPOP3.

Grids

The VPOP3 settings use grids in many places.

- You can sort grids by clicking on the column headers. Click twice to reverse the sort ordering.
- You can often edit grid entries by double clicking on the data you wish to change.
- In many cases, the grid will update immediately after you have made a change, without needing to press a **Submit** button.

Grid Filters

Many grids will have filter boxes visible just under the column headers. In some cases the boxes are always there, in other cases, there may be a button called **Show Filters** to display the filter boxes.

There are three types of filter boxes, depending on the data stored in the column.

- For most text columns, you can type text into the filter box. This will show any rows which contain that text as a substring.
- Some text columns with a limited choice of values will show a drop-down box from which you can select the value to display.
- For numeric columns you can either enter a specific number to search for, or use $>$, $<$, $>=$ and $<=$ operators to search for values matching the condition (e.g. >10 will match values greater than 10), or $x..y$ to search for values in the range x to y .

5.1 Users

The **Users** tab in the VPOP3 settings lets you manage the list of [Users](#) handled by VPOP3.

At the top of the page **(1)** is a count of the number of messages defined, and your licence limit (if your licence is unlimited, then the limit is not displayed).

Below that **(2)** are some buttons to perform actions which aren't specific to a single user:

- [Import users from file](#)
- [Import users from Windows](#)
- [Export users to file](#)
- [Bulk add users](#)
- [Edit user welcome message](#)
- [Send admin message](#)
- [Bulk edit users](#)

Under those buttons is a count of the messages waiting to be sent out (3), and a table showing all the Users defined in VPOP3 (4).

You can [view & delete messages waiting to be sent out](#) by clicking on any of the text in the **Outgoing Message Queue** line.

You can create a new user by pressing the [New button](#) (5) or pressing the [Bulk add users](#) button if you want to add lots of users at once.

You can [edit a user](#) by double-clicking on the user entry in the list. You can edit several users at once, which can make it easier to compare the settings of a couple of users.

You can [delete a user](#) by selecting the user entry in the list, and pressing the **Delete** button (6).

Note that it is currently not possible to rename a user. In most cases this is unnecessary as you can use [Aliases](#) to give a user different email addresses.

The screenshot shows the 'User Accounts' section with 2 users defined. A toolbar contains buttons for 'Import users from file', 'Import users from Windows', 'Export users to file', 'Bulk add users', 'Edit user welcome message', 'Send admin message', and 'Bulk edit users'. Below the toolbar is the 'Outgoing Message Queue' showing 0 messages. A table lists user accounts with columns for Account Name, Group, Inbox Messages, Mailbox Size, and Comments. The table contains two entries: 'karl' and 'Postmaster'. Red circles and arrows highlight specific elements: a circle around the user count (1), a circle around the management buttons (2), arrows pointing to 'New' (5) and 'Delete' (6) buttons, and a circle around the table (4).

Account Name	Group	Inbox Messages	Mailbox Size	Comme
karl		16	13.1kB	
Postmaster		0	0	

Table Columns

The table has several columns and symbols to help with visualising your users

- The left-hand column contains one or more icons (overlaid) which indicate the 'state' of the user account:
 - 🔑 - this shows that this user is an [administrator](#)
 - 🔧 - this shows that this user has an [autoresponder](#) defined, but the autoresponder is not currently active (e.g. date or time conditions do not currently match)
 - 🔑 - this shows that this user has an autoresponder defined, and the autoresponder is currently active
 - 📧 - this shows that this user has a [forward or assistant](#) defined
 - 🔒 - this shows that this user account is currently [locked out](#) from at least one IP address, due to too many failed login attempts

- The **Account Name** column shows the user (or account) name. If this is greyed out, then the account is currently disabled. To the right of this column are three icons which can be used for quick access to specific user settings:  takes you to the user's [Autoresponder](#),  takes you to the user's [Permissions](#), and  takes you to the user's [Aliases](#).
- The **Group** column shows which [Group](#) this user is a member of (if any).
- The **Inbox Messages** column shows how many messages are in this user's **Inbox** mail folder (note this is NOT the number of messages in their entire mailbox). To the right of this number is an icon of a waste bin (). If you click on this, then you can quickly delete all the messages from the user's **Inbox** folder. In VPOP3 Basic this operation is not reversible, but in [VPOP3 Enterprise](#), you can use the [Recycle Bin](#) facility to undelete messages if the Inbox is cleared by mistake.
- The **Mailbox Size** column shows the size of the user's entire mailbox (note this is NOT the size of the user's **Inbox** folder alone).
- The **Comments** column shows the administrator defined comments for the user.

Show Filters

The **Show Filters** button makes some boxes appear where you can search for users:

- Search for user name by entering a substring in the **Account Name** filter box
- Select a group from the **Group** filter box drop-down
- Search by number of messages in the Inbox by either entering a specific number, or you can use > or < operators to search for users with more or less than a certain number of messages (e.g. **>10** will search for users with more than 10 messages in their Inbox)
- Search by mailbox size by either entering a specific number of bytes, or use > or < operators to search for users with more or less than a certain number of bytes in their mailbox (e.g. **<1000000** will search for users with less than about 1MB in their mailbox). Note that MB/GB/kB are not currently supported in the search
- Search for comments by entering a substring in the **Comments** filter box

5.1.1 Adding a User

To add a [user](#), go to the [Users](#) tab in the VPOP3 settings and press the **New** button. If you want to quickly add multiple users, then you can use the [Bulk add users](#) button instead.

When you press the **New** button you will be taken to a short dialog where you can enter the basic settings for a user.

Add User Show Hints

Please enter the **username** for the user you wish to add. This username must be between 1 and 32 characters long and can contain numbers, letters, or the period, underscore or hyphen characters. It should *NOT* contain spaces or the @ symbol.

Usually the **username** for a person is used as the part of their email address before the @ symbol. Eg, if you have a person whose email address you wish to be *james@company.com*, it is simplest if you set their username to be *james*.

People can be assigned multiple email addresses by using **Mappings** to define 'aliases' for that user. In this case it is often best to use their 'main' name or their 'personal' name. Eg, if *james@company.com* could also be addressed as *sales@company.com*, it is best to use *james* as his username, and then create a Mapping to make *sales* into an alias for *james*.

Username: *

Password: * ?

Confirm Password: *

You can enter a short (up to 80 characters) comment about this user account below - this is entirely optional.

Comments:

Copy settings from:

Send Welcome message to new user

Enter the user name (or account name) in the **Username** box. Often this is the part of the user's email address which comes before the @ symbol, but you can define extra or alternate email addresses by using [Mappings](#) or [Aliases](#). The user name must contain between 1 and 32 characters, and can contain numbers, letters, the period (.), underscore (_) or hyphen characters (-). (Other characters are strictly allowed by the email standards, but VPOP3 restricts it to the most common subset of these, because attempting to use other characters can cause interoperability problems and user confusion). Note that usernames are not case sensitive, so the username *albert* is equivalent to the usernames *Albert*, *aLbErT* and *ALBERT*.

Enter the user's desired password in the **Password** box, and re-enter it into the **Confirm Password** box. The minimum password length is usually 5 characters, but this can be adjusted on the [Security Settings](#) page. The maximum length is 16 characters. You can use any character, except for a space character, in a password. However, if you use non-ASCII characters, then you may encounter interoperability issues - e.g. a £ character may be encoded as character 163 if sent using the [ISO-8859-1](#) character set, or as the characters 194, 163 if sent using the [UTF-8](#) character set. As passwords do not have any way of specifying a character set, you should try to avoid non-ASCII characters.

The **Comments** box can be used to contain any comments which you want to associate with the user account. This can be anything you wish, such as the user's real name, department, type of account etc. You can search or sort on this field in the **Users** list.

The **Copy Settings from:** ... setting lets you copy all settings (other than those entered in this dialog) from an existing user to the new user. If you want to create a user with the default settings, then simply leave this setting at the default **<None>** option.

An administrator can create a **Welcome Message** which can be sent to new users. If you have configured such a message, then the **Send Welcome message to new user** option will put the welcome message into the user's new **Inbox** folder.

5.1.2 Editing a User

To edit a user, double-click on the user name in the **Users** list. A window will appear with many tabs.

- [General](#)
- [Passwords](#)
- [Routing](#)
- [WebMail Settings](#)
- [Autoresponder](#)
- [Permissions](#)
- [Aliases](#)
- [Message Rules](#)
- [Quotas](#)
- Address Book
- [Outgoing Sig](#)
- [Internal Sig](#)
- [Advanced](#)
- Media
- [Prune Rules](#)
- [Folders](#)
- Finger Info
- Sender Address

You can edit several users at a time by double-clicking on their entries without closing the previous editing window. This lets you compare the settings of multiple users more easily.

5.1.2.1 General

The screenshot shows the 'Edit User - marc' window with the 'General' tab selected. The 'Primary Group' is set to '<None>'. The 'Secondary Groups' section has two lists: 'Selected Groups' (empty) and 'Available Groups' (containing 'office' and 'sasdadadsda'). The 'Comments' field contains 'aaaa'. The 'Account access allowed' checkbox is checked, while 'Administrator' and 'Account Locked Out' are unchecked. The 'Account expires at end' field is empty, with a note '(leave blank for no expiry date)' below it.

The user's **General** tab defines basic settings for the user.

Users can be in zero or more **Groups**. In VPOP3 a Group is a sort of **List** which is also used for assigning permissions and settings. If you are simply wanting a 'distribution group', then in VPOP3 add the users to a **Distribution List** instead. Doing this is done in the [List settings](#), not in the User settings.

The **Primary Group** allows you to override user settings by group if you wish. The Primary Group has settings such as permissions which can override individual user's settings. This means that you can change the settings for a group of users in one action rather than individually. However, note that the [Bulk Edit](#) option may achieve a similar result and be easier to understand in many cases. A user can only be in one **Primary Group**.

Secondary Groups do not allow you to override user settings but are used for permissions for IMAP4 folder sharing (and maybe used for other permissions in the future). A user can be in multiple **Secondary Groups**.

The **Comments** box lets you assign a comment to the user for future reference. This can be viewed in the [main Users list](#).

The **Administrator** box lets you indicate that this user is a VPOP3 administrator. Any user can be an administrator. Administrators have permission to log into the VPOP3 settings (using their own username & password details). When VPOP3 is first installed an initial administrator is created (usually called 'postmaster'). This initial user is no different from any other user who has been set as an administrator, so can be deleted in the future (you need to log in as a different administrator first, because an administrator cannot delete themselves or set themselves to not be an administrator).

The **Account Locked Out** box cannot be checked manually. If VPOP3 [detects several bad login attempts](#) from an IP address it will lock the account for a period of time so that it cannot be logged into from that IP address. In that case the **Account Locked Out** box will be checked and VPOP3 will display the locked IP addresses. You can uncheck the box and press **Submit** to remove the account locks.

Note - if the account is locked, any attempts to login will result in a generic 'Login failed' type error message. If you get a **Mailbox Locked** error when trying to login using POP3 or IMAP4, that does *not* mean that the account is locked. Each mailbox has an exclusive-access lock which is required to meet the POP3 standards, any POP3 client will attempt to acquire this lock and the first IMAP4 client to access the mailbox will also attempt to acquire this lock. **Mailbox Locked** means that this exclusive-access lock has already been acquired by another email client. Check the [Status → Active Sessions](#) view to see which other computer is already logged into the mailbox. The lock is released when the POP3 client logs out, or the last IMAP4 client logs out.

The **Account access allowed** box means that the account is active. If you want to disable the account then uncheck the box (incoming mail to the mailbox will still be accepted, but the user will not be able to collect it or perform any other actions which require them to log in). The only exception is that if the user is a VPOP3 administrator, they will be able to log into the Web interface (this is to prevent you accidentally locking yourself out). If you stop the user being an administrator as well, then they won't be able to log into the web interface either.

The **Account expires at end** box lets you set an expiry date for the account (for instance for temporary accounts). The account will become inactive at the end of the specified day. It will *not* be deleted at that time. If you click on this box a calendar will be displayed so you can select a date.

Inactive accounts are displayed in grey on the [main Users list](#).

5.1.2.2 Passwords

Submit

Prune Rules	Folders				Finger Info	Sender Address	
Message Rules	Quotas	Address Book	Outgoing Sig	Internal Sig	Advanced	Media	
General	Passwords	Routing	WebMail Settings	Autoresponder	Permissions	Aliases	

Passwords must have at least 3 characters, and may not contain spaces.

Main Password :
 Generate Display

Confirm Main Password :

Web Password :
 Generate Display

Confirm Web Password :

Have different 'Main Password' and 'Web Password'

User can change Main Password through WebMail

Email for password resets :

The user's **Passwords** tab lets you set the passwords for the user and some password-related settings.

The **Main Password** is the password used by SMTP, POP3 & IMAP4 email clients. It is also used for Webmail & administrator logins if the **Have different 'Main Password' and 'Web Password'** option is not checked.

The password has to be at least a certain length. This minimum length is set in the [security settings](#). The password cannot contain spaces but can contain any other character. No other checks (eg password strength checks) are performed by VPOP3 by default. It is possible to have a Lua script to check whether a new password is suitable.

The **Generate** button will make VPOP3 generate and display a random password. The **Display** button will display a password as it is being entered. It will *not* display a previously-entered password.

The **Web Password** options are the same as for the **Main Password** and are enabled if the **Have different 'Main Password' and 'Web Password'** option is checked.

The **Have different 'Main Password' and 'Web Password'** option lets you indicate that the Webmail & administrator password is different from the POP3/SMTP/IMAP4 password. This can be used if a very secure and not-memorable password is set for the POP3/SMTP/IMAP4 password, is programmed into email clients and the administrator does not want the user to be able to change it. The user should never need to re-enter this password once it has been configured into the email client software so, in some environments, the user may not even know what this password is. Users may still need to be able to log into Webmail so the password for that may need to be more memorable and the user may wish to reset this password, so allowing the passwords to be different will allow this password to be reset without stopping the email client from logging in.

If the **User can change Main Password through WebMail** option is checked then the user can change their **Main Password** through Webmail even though they are logging in with a different Webmail password. If the **Main Password** is the same as the **Web Password**, then the user can always change that password, and if the two passwords can be different, then the user will always be able to change their **Web Password**. *There is no way to prevent the user from changing the password they use to log into Webmail.* This is deliberate because that password is more likely to be compromised if the user has to remember and enter it.

If a user forgets their password they can ask for a password reset email on the Webmail login page. By default this password reset email will be sent to their VPOP3 mailbox. If they have [message forwarding](#) set up then this message will be forwarded as normal, or if their email client is still configured with a correct password they will be able to see the password reset email. However, in other cases they will not be able to access the password reset email, because they will need to know the password to be able to access the email. So, if you put an alternative email address in the **Email for password resets** box, then password reset email will be sent to this alternative email address instead of into the VPOP3 mailbox.

If all VPOP3 administrators have forgotten their passwords, then see the **Lost Administrator Password** topic for help.

Important note when changing passwords

When changing passwords in VPOP3 it is important to note that the security features of VPOP3 can cause problems. Often email clients or mobile devices will try to log into VPOP3 periodically. If you change the password in VPOP3, then these devices will attempt to log in with the old (now incorrect) password until the password is changed in those as well. This can cause VPOP3 to [lock accounts](#) or [block IP addresses](#).

If you cannot stop email clients from attempting to log in, it can sometimes be worth temporarily increasing the attack detection thresholds in VPOP3. If you go to the **Security Settings** in VPOP3, and increase the **Lock user after** value on the **General** tab and the **Failed login threshold** on the **Intrusion Protection** tab, eg to 1000, then that should prevent VPOP3 from blocking the account or IP address. Remember to reset the security settings back to their previous values afterwards.

5.1.2.3 Routing

Changes have been made - press: Submit

Prune Rules	Folders				Finger Info	Sender Address	
Message Rules	Quotas	Address Book	Outgoing Sig	Internal Sig	Advanced	Media	
General	Passwords	Routing	WebMail Settings	Autoresponder	Permissions	Aliases	

Message Routing

Assistant : i

Redirect to assistant (don't keep a local copy)
 Immediately copy messages already in this user's inbox to assistant(s)

Forward To : i

Use Forwarding
 Don't use forwardings or assistants if mail would be quarantined

Copy Sent Messages To: i

In the settings below, enter dates as YYYYMMDD and times as HH:MM. Note that if you specify both date and time, it will use the time conditions on the specified days. For instance "20070101 10:00 to 20070108 12:00" means "from 10:00-12:00 on 1st to 8th (inclusive) of January 2007".

Use Assistants between : and (leave blank for always)

Use Forwards between : and (leave blank for always)

Edit Routing Script

Size Dependent Forwarding i

If message >= **kB** Copy **to**

If message <= **kB** Copy **to**

The user's **Routing** tab lets you set the how incoming messages will be handled - eg message forwarding.

The **Assistant** is a list of email addresses to whom incoming messages to this mailbox will be copied (unless **Redirect to assistant** is checked). You can specify multiple assistants by separating their email addresses with a semicolon. If the assistant is another local VPOP3 user, you can just specify the user name; you don't need to specify the full email address (the full address will still work).

Also, if the message is coming FROM one of the Assistant addresses, then VPOP3 will ignore the Assistant setting. This is deliberate functionality. This is so that, for instance, you can set Joe to be the Assistant for Kate, and have incoming messages for Kate redirected to Joe. So, all messages addressed to Kate can be checked by Joe first. Then, if Joe forwards a message on to Kate, VPOP3 will see that the message is coming from the Assistant, so will not redirect it back to Joe, but will let the message be delivered to Kate.

Also, note that if the Assistant also has an Assistant defined, the message will be sent to the Assistant, but *not* to the Assistant's Assistant (this is to try to avoid unexpected loops or message 'explosions').

Usually the Assistant function will send a copy of the message to the specified address(es). However, if the **Redirect to assistant** box is checked, then VPOP3 will redirect the message to the Assistant(s) and this user will not receive a copy of the message.

If the **Immediately copy messages already in this user's inbox to assistant(s)** box is checked, then VPOP3 will immediately copy any messages in this user's inbox to any local assistants specified. (The setting in this box is not remembered, so must be checked to cause this action). This can be useful if you set the assistant 'too late' and some messages have already been received by the user but weren't copied or redirected to the assistant.

The **Forward To** is a list of email addresses to whom incoming messages must be redirected. You can specify multiple assistants by separating their email addresses with a semicolon. If the assistant is another local VPOP3 user, you can just specify the user name; you don't need to specify the full email address (the full address will still work). If you have a **Forward To** address set, then this user will not receive a copy of the message as well, the messages will only be forwarded. You can use the **Assistant** and **Forward To** options together, but you cannot use the **Redirect to assistant** option with **Forward To**.

The **Use Forwarding** box lets you enable/disable the **Forward To** addresses in one step. This means the addresses do not have to be deleted (and possibly forgotten) if you want to temporarily disable forwarding.

The **Don't use forwardings or assistants if mail would be quarantined** box lets you tell VPOP3 that if the message would be quarantined it should not be forwarded. If this box is not checked, then potential spam will be forwarded along with other mail. If the target users are local VPOP3 users, then the spam messages will be placed into the target users' [spam quarantines](#), but if the target users are not local VPOP3 users, the spam messages will be forwarded to them. This may make the mail server for the remote users think that VPOP3 is sending spam, so it may restrict or block it from sending mail. If this box is checked, then VPOP3 will place the potential spam in this user's spam quarantine, and it won't be forwarded at all.

The **Copy Sent Messages To** setting lets you specify addresses to whom messages sent by this user should be copied (BCCd). You can specify multiple addresses by separating them with semicolons. If you want to use this option your users should use [SMTP authentication](#) when sending messages.

Routing Script Settings

The next section is actually handled by the Routing script. By default a basic routing script is installed. The script can be changed to change how the settings are presented and how they behave. The description below is for the default routing script. If it is different for you, then you may have a different routing script.

The **Use Assistants between** and **Use Forwards between** settings let you specify the times and dates when the **Assistant** and **Forward To** settings will apply. Specify any dates as **YYYYMMDD** and times as **HH:MM** (24 hour clock server local time). For instance, you could specify **12:00** for a time or **20161013** for a date or **20161013 12:00** for a date and time. If you specify both date and time, then the script treats them separately, so **20161013 12:00 to 20161017 15:00** means from 12 noon until 3pm on 13th, 14th, 15th, 16th and 17th October; it does not mean from 12 noon on 13 October until 3pm on 17 October.

Size Dependent Forwarding

Size Dependent forwarding lets you configure forwarding rules depending on the size of the message.

The first one lets you specify that if a message is larger than a certain size it can be copied or redirected to specified email addresses (separate multiple addresses with semicolons). The second one lets you specify that if a message is smaller than a certain size it can be copied or redirected.

To disable an option simply set the size to 0 or the target addresses to blank.

Caution

Because of spam, many mail servers are suspicious of forwarded mail, so you may find that forwarding to external addresses does not work reliably, especially to some of the large mail service providers who may block, reject or quarantine forwarded mail. This can be because spam is being forwarded which reduces the reputation of your server, or because the mail is appearing to come from one email address but is not coming from a server associated with that email address. In most cases it is better either for the user to collect the mail from the VPOP3 mail server over the Internet, or, if possible, have the mail service provider collect the mail from the VPOP3 mail server over the Internet (eg [Gmail - check email from other accounts](#))



Tip

Forwarding and Assistants from VPOP3 do NOT change the recipient and sender addresses in the message headers. The message will still appear to be from the original sender, and to the original recipient.

This can occasionally cause confusion where someone may be uncertain why they received a particular message. The [Message Trace](#) function may help establish why the message was received in this case.

5.1.2.4 WebMail Settings

WebMail Real Name :

WebMail Email Addresses :
(One per line)

These are email addresses which this user can use for sending messages through the VPOP3 WebMail server.

The user can change this setting through the WebMail "WebMail Settings" page. If you want to disable that facility for your users, you can change the "**Allow WebMail email address settings**" option on the [Services -> WebMail](#) settings page.

Allow Message Move to : (Can be a user, group or distribution list - if it is a group/list, then the user will be able to choose which member of the group/list to move the message to)

Move directly to destination user, disregarding mappings etc (only allows moving to local users)

Allow user to change autoresponder via WebMail

Allow user to change forwards/assistants via WebMail

Users can set forwards to these addresses :

Disable links in messages

Allow user to view images in WebMail

Allow user to change names of special folders in WebMail

Allow user to change their 'Real Name' setting in WebMail

Allow user to change actions on quarantine message release in WebMail

On Webmail Quarantine Release, add to whitelist

On Webmail Quarantine Release, train Bayesian filter

On Webmail Quarantine Release, report false positive

Allow user to create calendars in WebMail

Allow user to share calendars in WebMail

Allow user to see global address book entries

Allow user to access message archive ⓘ

The user's **Webmail Settings** tab defines settings for VPOP3's Webmail for this user.

WebMail Real Name is the name used as the sender's name when sending messages from VPOP3's Webmail.

WebMail Email Addresses is a list of email addresses which this user can select from when sending messages from VPOP3's Webmail. If the box is blank, then only the sender's main email address (as defined in the **Address Book** tab) can be used, otherwise any of the email addresses listed here can be selected. The user can edit these addresses themselves in their Webmail settings, unless you disable the **Allow WebMail Email Address Settings by users** in [Services -> WebMail -> WebMail Settings](#).

The **Allow Message Move to** option allows the user to move a message to the selected user(s) from within Webmail. If you choose a group or list here, then the user will be able to select which group/list

member the message is to be moved to. If you choose a user here, then the message can only be moved to that user.

The **Allow user to change autoresponder via WebMail** option allows the user to modify their own [autoresponder](#) from within Webmail.

The **Allow user to change forwards/assistants via WebMail** option allows the user to modify their own forwarding & assistant settings.

The Users can set forwards to these addresses option indicates which email addresses the user can set their forwarding & assistant settings to via Webmail. This is either a [regular expression](#) or a [wildcard](#) address. Only one entry can be specified here, so you could use a specific email address or a wildcard expression like `*@mydomain.com` or a regular expression line `/^(bob|kate|joe)@mydomain\.com$/`. If this is blank, then any address can be specified.

The **Disable links in messages** option means that any links in email messages displayed in Webmail are disabled and will not work. If this option is not checked, then links will work as normal. This option can be useful if users are not very careful about what they do.

The **Allow user to view images in WebMail** option allows the user to view images in email messages in Webmail. If this option is not checked, then placeholders are displayed instead. This may make some messages harder to read, but will prevent inappropriate images or tracking images being displayed.

The **Allow user to change names of special folders in WebMail** option allows the user to change which folder will be the 'deleted items' or 'sent items' folders. Usually this is OK, but it can be useful to disable this if you have a user who sets them inappropriately or to make support easier sometimes.

The **Allow user to change their 'Real Name' setting in WebMail** option allows the user to change their real name on sent messages from Webmail. You may want to restrict this to prevent users pretending to be someone they are not.

The **Allow user to change actions on quarantine message release in WebMail** allows the user to change whether sender addresses are added to the spamfilter whitelist etc when releasing messages from the quarantine via Webmail.

The **On Webmail Quarantine Release, add to whitelist/train Bayesian filter/report false positive** options set the default options for when releasing messages from the quarantine. If the above **Allow user to change actions on quarantine message release in WebMail** option is checked, then the user can change these options if they wish for each message they release.

The **Allow user to create calendars in Webmail** option (only in VPOP3 Enterprise) means that the user can create extra CalDAV calendars in Webmail. Some administrators wish to turn this off to have more control over what users do.

The **Allow user to see global address book entries** option allows the user to see global address book entries (including local users, lists etc). In some cases it can be a good idea to turn this off so that the user can only see their personal address book, or address books which have been explicitly shared with them. For instance, if you have a shared server used by multiple organisations it may be undesirable for users to be able to see all other users on the server.

The **Allow user to access message archive** option lets the user search and view [archived messages](#) from within Webmail. Normally only administrators can access the archive through the settings, but if this option is checked, the user can search the archive for messages sent by, or received by themselves.

5.1.2.5 Autoresponder

Submit

Prune Rules	Folders				Finger Info	Sender Address	
Message Rules	Quotas	Address Book	Outgoing Sig	Internal Sig	Advanced	Media	
General	Passwords	Routing	WebMail Settings	Autoresponder	Permissions	Aliases	

Autoresponders

Name	Log Entries
Summer Holiday	0

Add Autoresponder Edit Autoresponder Delete Autoresponder View Log Clear Log

Import Export

Rules

Name	Responder	En	Lo	Matches	Date	Time	DateTime	Days Of Week	Sender	Subject
Default for Sum	Summer Holid	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	2016-08-01-2016-08-14	-	-	SuMoTuWeThFrSa		

Add Rule Edit Rule Delete Rule Move Rule Up Move Rule Down

Header filters and triggers

Below, you can specify header filters and triggers. These match against the incoming message header.

If a filter matches the incoming header, then the autoresponder will not trigger.

If a trigger matches the incoming header, then the autoresponder will trigger (unless it is also filtered by a filter). If no triggers are specified, then VPOP3 acts as if a generic trigger which matches all messages is present.

Triggers and filters are specified as **<Header field> ":" <Data to match>**, eg "Subject: no response*". You can use * and ? wildcards in both triggers and filters.

Header Filters :

(These filters are added to the ones on the general Settings -> Autoresponder Settings page)

Header Triggers :

The user's **Autoresponder** tab defines autoresponders for this user. An autoresponder is an email which is automatically sent when a message arrives in a user's mailbox.

It is important to note that autoresponders will only trigger if a message actually arrives in a user's mailbox. If [Mappings](#) or [forwards](#) mean that the message gets delivered elsewhere, then the autoresponder will not trigger even if it was originally addressed to this user.

In VPOP3, there are Autoresponder Rules and Autoresponders themselves.

When a new message arrives in the user's Inbox, VPOP3 checks for autoresponders as below:

1. The **Header Filters** are checked. If the incoming message header matches the Header Filters, then no autoresponder is triggered.
2. The **Header Triggers** are checked. If there are no Header Triggers or the incoming message header matches the Header Triggers, then VPOP3 continues to step 3. Otherwise no autoresponder is triggered.
3. The **Autoresponder Rules** are checked one at a time. If the incoming message and date/time match an autoresponder Rule, then the autoresponder associated with that Rule is triggered and the processing stops. Otherwise the next Rule is checked until one matches or all the Rules have been checked.

Autoresponders

The **Autoresponders** section defines autoresponder messages & actions when an Autoresponder Rule is triggered.

You can add, edit and delete Autoresponders by pressing the **Add Autoresponder**, **Edit Autoresponder** and **Delete Autoresponder** buttons respectively. You can also edit an Autoresponder by double-clicking it in the list.

Each time an Autoresponder is triggered, VPOP3 logs this. You can view the log for an autoresponder by selecting it and pressing the **View Log** button. You can clear the log by pressing the Clear Log button. (Entries are automatically deleted from the log after 180 days or when the Autoresponder definition is deleted).

The **Export** button exports the selected Autoresponder definition to a file, and you can re-import it later by using the **Import** button.

See also: [Editing/Adding an Autoresponder Definition](#)

Autoresponder Rules

The Autoresponder **Rules** section defines Autoresponder Rules which tell VPOP3 what the conditions are for triggering autoresponders. The Rules list is ordered - VPOP3 will check it from top to bottom until it finds a rule which matches, and then it won't check any further rules.

You can add, edit and delete Autoresponder Rules by pressing the **Add Rule**, **Edit Rule** and **Delete Rule** buttons respectively. You can also edit an Autoresponder Rule by double-clicking it in the list. You can re-order Rules by selecting them and pressing the **Move Rule Up** and **Move Rule Down** buttons.

If a Rule is greyed out in the list, then it means that it is not enabled, so VPOP3 will ignore it when checking for matching Rules.

See also: [Editing/Adding an Autoresponder Rule](#)

Header Filters and Triggers

Autoresponder Header Filters and Triggers let you tell VPOP3 when autoresponders will or will not be used. These are checked before the Autoresponder Rules so will affect all Autoresponders for this user. You can also global autoresponder filters in [Settings -> Autoresponder Settings](#) which apply to all VPOP3 users.

The **Header Filters** box lets you specify data to look for in the message header of the incoming message. If any headers match, then no autoreponse will be triggered,

For example: **Subject: NoReply*** looks for the **Subject:** line in the message header and checks if the data for that header field begins with **NoReply**. VPOP3 does a case-insensitive check and allows [wildcards](#).

The **Header Triggers** box lets you specify data to look for in the message header of the incoming message. If any headers match, then the autoreponse will be triggered, If there are no Triggers defined, then VPOP3 will act as if a generic trigger matched.

For example: **From: *@customer.com*** looks for the **From:** line in the message header and checks if the data for that header field contains **@customer.com**. VPOP3 does a case-insensitive check and allows [wildcards](#).

Put each filter or trigger condition on a line of its own. If *any* of the list of conditions match, then VPOP3 treats that section as matched.

Also be aware that the filter & trigger conditions have to match exactly (with wildcard checking and case insensitivity).

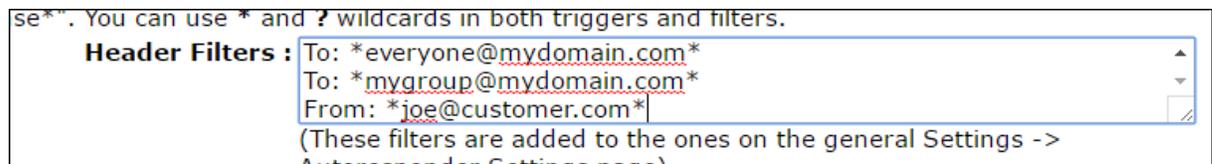
From: joe@customer.com

will only match if the From header field is *exactly* **joe@customer.com**. If the From header field is something like:

From: "Joe Brown" <joe@customer.com>

then it will *not* match, because you have told VPOP3 that it has to *exactly* match **joe@customer.com**. Use wildcards if you want to test for text being included in the header line.

Example:



Note that in most cases, it is best to leave the **Filters & Triggers** fields blank and use [Autoreponder Rules](#) instead.

5.1.2.5.1 Edit Autoresponder Definition

Edit Autoresponder

Close **Changes have been made - press:** Submit

Autoresponder Name : 

Keep Original Message 

Response Text:

I will be on holiday from 1st until 15th August and will reply when I return

Advanced Settings

Copy original message to : 

Don't send to same sender within :  hours

Autoresponder From address : 

Autoresponder Reply-To address : 

Autoresponder Subject Prefix 

Append Original Message : 

Send response to : 

Send response to original sender 

Attachments :
(This is the list of available attachments - select the attachments you want to include with this autoresponse message)  (Use Ctrl+Click for multiple select)

New Attachment: No file chosen

This window lets you define an Autoresponder for a user. To get here [edit a user](#), go to the [Autoresponder](#) tab and add or edit an Autoresponder.

The Autoresponder definition tells VPOP3 *what* to do when it automatically responds to an incoming message. To define *when* VPOP3 should automatically respond to an incoming message, see the [Autoresponder Rule settings](#).

The **Autoresponder Name** is a name you give to the Autoresponder definition for your future reference. It can be anything you wish.

The **Keep Original Message** option tells VPOP3 to leave the original incoming message in the user's Inbox after responding to it. *Usually this should be checked*. If it is not checked, then the original message is discarded after responding. This can be useful if the mailbox is only used for automatic responses - for instance, people can email to the mailbox to automatically receive a specific document by reply.

The **Response Text** is the autoresponder text message. This is usually plain text, but advanced users can specify HTML by specifying HTML source code surrounded by <HTML> and </HTML> tags. You can also specify text replacements - see below for more information.

The **Advanced Settings** can be left unchanged in most cases but they make some things possible that would not otherwise be so.

The **Copy original message to** option tells VPOP3 to copy the original incoming message to the specified email addresses (separate multiple addresses with semicolons, commas or spaces). This can be used to redirect (if 'Keep Original Message' is unchecked) or copy (if 'Keep Original Message' is checked) the incoming message to another user whilst the Autoresponder is active. Note that this option is still processed, even if an automatic response is not sent due to the 'Don't send to the same sender' option below.

The **Don't send to same sender within X hours** option tells VPOP3 not to send this autoresponder to someone it has already sent it to within the past X hours. This is useful to prevent autoresponder loops where two users' autoresponders constantly reply to each other. We recommend that this option is set to a non-zero value.

The **Autoresponder From Address** option tells VPOP3 where the autoresponder should appear to come from. If this is left blank, then VPOP3 will use the user's email address from their Address Book entry, or, failing that, it will use <username>@<default domain>. You can specify a text name in this field as well - eg: *Fred Bloggs <fred@example.com>*. This setting supports text replacements (see below).

The **Autoresponder Reply-To Address** option tells VPOP3 where replies to the autoresponder message should be sent. If this is left blank, then it will be set to *no-one@<default domain>* to try to prevent responses to the autoresponder message. If it is set to something, then a "*" character will be replaced with the username of this user. This setting supports text replacements (see below).

The **Autoresponder Subject/Subject Prefix** option tells VPOP3 either to set the autoresponder subject to the specified text, or to add a prefix (eg 'Re:') onto the original message subject. This setting supports text replacements (see below).

The **Append Original Message** option tells VPOP3 to add the original message onto the autoresponder. You can choose not to add the original message, or just to add the original message headers, or to add the entire original message.

The **Send Response to** option tells VPOP3 to send the automatic response to the specified email addresses (separate multiple addresses with semicolons, commas or spaces). This could be useful if you want someone to be notified of incoming messages to a user. If this is blank or the **Send response to original sender** option is checked, then the message will be sent to the original message's sender as well. (VPOP3 will use the Return-Path if [standard RFC 3834 behaviour is enabled](#), or the Reply-To address otherwise). This setting supports text replacements (see below).

The **Attachments** section lets you specify attachments to be added to the automatic response if you wish. (You can add attachments here, but full management of the uploaded attachments is performed on the **Media** tab).

Replacement text strings

Autoresponders support replacement text strings. This allows the creation of more generic automatic responses

For instance the response text: I am on holiday from {StartDate} to {EndDate}

will automatically replace the {StartDate} and {EndDate} with the start and end dates of the matching Autoresponder Rule, so the response may actually say "I am on holiday from 1 August 2016 to 15 August 2016" (or whatever dates are defined in the Autoresponder Rule).

Custom Replacements

To create a custom replacement, specify text in the appropriate setting like {\$....}. Then, in the Autoresponder Rule which triggers this Autoresponder, you will be given the option to specify data for these replacements, so if you specify {\$myname} in the Response Text, then the Autoresponder Rule will ask you for the value of 'myname'.

The data inside the braces must begin with a \$ character to indicate that it's a custom replacement, then the first character of the replacement name must be an alphabetic character, then you can continue the replacement name with alphanumeric characters. You can specify a default value by adding "("<default value>)" after the name.

For example: **{\$event(holiday)}** will create a custom replacement called 'event' whose default value is 'holiday'.

The **Autoresponder Reply-To Address**, **Copy original message to** and **Send Response To** fields only support Custom Replacements.

Built-in Replacements

The **Response Text**, **Subject Prefix**, **Subject** and **Autoresponder From Address** fields support the above Custom Replacements as well as a large set of built-in replacements.

In these fields, a \ character can be used to mean the next character must be included as-is, so \\ will include a \ character, and \{ will include a { character, not start a replacement tag.

Standard Replacements

Standard Replacements are specified like {<name>}.

The possible <name> values are

- **User** - the username whose responder is triggering.
- **Originator** - the email address of the incoming message's sender.
- **Subject** - the autoresponder subject.
- **OrigSubject** - the original incoming message's subject.
- **Date** - the date now using the current locale's default date format.
- **LongDate** - the date now using the current locale's default 'Long date' format.
- **ShortDate** - the date now using the current locale's default 'Short date' format.

- **Time** - the time now using the current locale's default time format.
- **TimeNoSecs** - the time now using the current locale's time format without seconds.
- **ConditionName** - the name of the Autoresponder Rule which matched.
- **ConditionDateFrom** - the value of the Autoresponder Rule's 'Date From' field.
- **ConditionDateTo** - the value of the Autoresponder Rule's 'Date To' field.
- **ConditionTimeFrom** - the value of the Autoresponder Rule's 'Time From' field.
- **ConditionTimeTo** - the value of the Autoresponder Rule's 'Time To' field.
- **ConditionDateTimeFrom** - the value of the Autoresponder Rule's 'Date/Time From' field.
- **ConditionDateTimeTo** - the value of the Autoresponder Rule's 'Date/Time To' field.
- **ConditionDOW** - the value of the Autoresponder Rule's 'Days of Week' field.
- **ConditionMatches** - the value of the number of times the Autoresponder Rule has matched.
- **StartDate** - the start date of the Autoresponder Rule (based on Date From & Date/Time From fields).
- **StartDate-1** - the day before **StartDate**.
- **EndDate** - the end date of the Autoresponder Rule (based on Date From & Date/Time From fields).
- **EndDate+1** - the day after **EndDate**.
- **Date:<format>** - the date now using the specified format
- **StartDate:<format>** - the start date using the specified format
- **StartDate-1:<format>** - the day before the start date using the specified format
- **EndDate:<format>** - the end date using the specified format
- **EndDate+1:<format>** - the day after the end date using the specified format
- **Time:<format>** - the time now using the specified format

If a Date Format includes a % character, then it is as specified [here](#), otherwise it is as specified [here](#).

If a Time Format includes a % character, then it is as specified [here](#), otherwise it is as specified [here](#).

Control Replacements

Control Replacements are specified like {<statement>}. They let you include parts of the autoresponder depending on Custom Field values

- **{if \$<name>}** - include the following text (until **{else}** or **{endif}** is found) if the specified custom field exists and is not empty. Otherwise, include the text after the subsequent **{else}** if any.
- **{ifnot \$<name>}** - include the following text (until **{else}** or **{endif}** is found) if the specified custom field doesn't exist or is empty. Otherwise, include the text after the subsequent **{else}** if any.
- **{rem }** - a comment

For example

```
{if $bibble}
Bibble is not empty
```

```
{else}
Bibble is empty
{endif}
```

Lua Replacements

If you specify `<lua>...</lua>` then VPOP3 processes the text between the `<lua>` tags as a Lua script, and the 'print' output of the script is placed in the Response Text instead.

The Lua script will have global variables of:

- all the standard built-in replacements above.
- the custom replacements called 'customfield_<name>'.
• a global string called 'Message' which contains the original incoming message content
- a global Lua table called 'Autoresponder' will autoresponder behaviour settings. The script can change some of these if it wishes.

The *Autoresponder* table has the values:

- **ID** - autoresponder ID (readonly)
- **OwnerID** - autoresponder owner user ID (readonly)
- **Name** - autoresponder **Name** value (readonly)
- **Text** - autoresponder **Response Text** value (readonly)
- **Keep** - (boolean) - **Keep original message** value
- **Checklog** - (number) - **Don't send to same sender within X hours** value
- **Sender** - **Autoresponder From address** value
- **ReplyTo** - **Autoresponder Reply-To address** value
- **Subject** - **Subject** value
- **SubjectPrefix** - **Subject prefix** value
- **AppendMsg** - (number) **Append Original Message** value (0 = No, 1 = Headers, 2 = Full)
- **To** - (table) list of **Send Response To** addresses
- **CopyTo** - (table) list of **Copy original message to** addresses
- **Attachments** - (table) list of **Attachment** names

5.1.2.5.1.1 Edit Autoresponder Rule

Edit Autoresponder Rule

Close Submit

Rule Name :

Autoresponder : i

Enable this rule i

Prevent user changes for this autoresponder i

Conditions

Specify the conditions below to make this autoresponder trigger. Leave conditions blank if you do not want that data tested. Leaving all entries blank will make the autoresponder always trigger.

All the dates/times below are specified in the server's local time zone

Dates : x To i x

Times : To i

Date/Time : x To x i

Days of the Week : Sun Mon Tue Wed Thu Fri Sat i

Sender : i

Subject : i

This window lets you define an Autoresponder Rule for a user. To get here [edit a user](#), go to the [Autoresponder](#) tab and add or edit an Autoresponder Rule.

The Autoresponder Rule definition tells VPOP3 *when* to use an autoresponder. To define *what* VPOP3 should do, see [Autoresponder Definition settings](#).

VPOP3 processes the list of Autoresponder Rules in order from top to bottom and stops when it finds a matching rule, so you can use Rules to prevent other autoresponders from being triggered. You can alter the order of the Rules on the main Autoresponder tab.

The **Rule Name** is a name you specify for the rule. It can be anything, but we suggest something meaningful so it will help you maintain the settings.

The **Autoresponder** option sets the Autoresponder definition which will be used when this rule is triggered. You can choose **<None>** here so that no autoresponder is triggered when the rule matches. This can be useful to set exceptions to other autoresponders.

The **Enable this rule** box lets you easily enable or disable this rule without having to totally remove it.

The **Prevent user changes for this autoresponder** means that the user cannot change the rule from their Webmail settings.

The **Conditions** section sets which conditions need to match for the Autoresponder Rule to be triggered. Any conditions which are left blank will not be checked and will be deemed to always match. So, if you create a rule and just leave all the conditions blank/as default, then the Autoresponder Rule will match any incoming message.

The **Dates** settings tell VPOP3 between which dates the Rule should be triggered. The dates are inclusive and start/end at midnight. The dates are shown in YYYY-MM-DD format. So, 2016-08-01 to 2016-08-14 means that the Rule will be triggered from 00:00 on 1st August 2016 until 24:00 on 14th August 2016 (or 00:00 on 15th August 2016).

The **Times** settings tell VPOP3 between which times the Rule should be triggered. The times are inclusive and are in 24 hour format. You can select times in 15 minute segments. So 8:15 to 14:45 means that the Rule will be triggered from 8:15 am until 2:45 pm each day.

The **Date/Time** settings tell VPOP3 between which dates & times the Rule should be triggered. The dates are inclusive. The dates are shown in YYYY-MM-DD format. So, 2016-08-01 8:15 to 2016-08-14 14:45 means that the Rule will be triggered from 8:15 am on 1st August 2016 until 2:45 pm on 14th August 2016.

Note that using the **Dates** and **Times** settings together is different from using the **Date/Time** settings.

If you set **Dates** to be 2016-08-01 to 2016-08-14 and **Times** to be 8:15 to 14:45, then the Rule will be triggered between 8:15 am and 2:45 pm on each day from 1st August 2016 until 14th August 2016. (So, for instance for a message arriving at 5:00am on 5th August it *will not* be triggered)

If you set **Date/Times** to be 2016-08-01 8:15 to 2016-08-14 14:45, then the Rule will be triggered between 8:15 am on 1st August 2016 until 2:45 pm on 14th August 2016. (So, for instance for a message arriving at 5:00am on 5th August it *will* be triggered)

The **Days of the Week** settings specify which days of the week you want the Rule to be triggered. For instance, you could use this to have a different rule to be triggered on week days from at weekends.

The **Sender** setting lets you specify the sender email address which has to match to trigger this Rule. You can use [wildcards](#) and [regular expressions](#) (by surrounding the text with / characters). For instance, you could use something like `*@my.local.domain` to create a rule specific to local mail so that this triggers a different autoresponder or prevents an autoresponder at all (using **<None>** in the Autoresponder setting).

The **Subject** setting lets you specify the subject line which has to match to trigger this Rule. You can use [wildcards](#) and [regular expressions](#) (by surrounding the text with / characters).

5.1.2.6 Permissions

Allowed Protocol : POP3 Server
 IMAP4 Server
 SMTP Server
 WebMail Server
 Password Server
 LDAP Server

Max outgoing message size : 0 kB (0 = no limit)

Put user in *Everyone* list

Allow sending of Internet mail

Allow receiving of Internet mail

Monitor Messages (See Settings -> Message Monitoring - only used if a **What to monitor** option is set to **Selected**)

Allow sending BCCs

Default IMAP4 Folder permissions : Full permissions

Remote Status Server Permissions

Allow user to view connection status
 Allow user to view total queue message counts
 Allow user to view user queue message counts
 Allow user to view server activity log
 Allow user to initiate connections on server
 Allow user to shutdown the server (not recommended for non-administrators)
 Allow user to receive instant messages
 Allow user to send instant messages

The user's **Permissions** tab defines the permissions for the user.

The **Allowed Protocol** section let you set which Internet protocols can be accessed by this user (the IMAP4 option in the screenshot above is only available in VPOP3 Enterprise). By default, a user can access all protocols supported by VPOP3. If you disable access for a specific protocol, then if the user tries to log in using that protocol their login attempt will be treated as if the user does not exist.

This option can be useful in several cases. For instance, if you have VPOP3 Enterprise you may decide that some users have to use POP3 instead of IMAP4, or vice versa, so you can enforce that by disabling the relevant protocol. Or, you may have a user account which is just used for collecting mail, so you could disable the SMTP protocol for that user.

Note that the [IP Access Restrictions](#) for the services take precedence over the protocol permissions here, so, for instance, even if the POP3 protocol is allowed here, if the IP access restrictions don't allow POP3 access from a certain IP address, the user won't be able to access VPOP3 using the POP3 protocol.

The **Max outgoing message size** sets the maximum size of outgoing messages sent by this user (if they send using SMTP authentication). Larger messages will be rejected by VPOP3. There are other places where size restrictions can be made - the [SMTP Service General](#) tab, in [SMTP Rules](#), or in [Group settings](#) if the user is in a VPOP3 group. The user should receive an error message in their email client software if they try to send a message which is too large.

The **Put user in Everyone list** option lets you remove the user from the built-in list **Everyone**. This can be useful if you use that list to send messages to all your users and you have a mailbox used for a device (such as a network printer) or resource and you do not want to send messages to that mailbox when sending them to "everyone".

The **Allow sending of Internet mail** option lets you indicate whether this user can send messages to remote email addresses. If you want to restrict a user to only sending messages to other users on this VPOP3 server, then remove the check from this box. If Internet mail *is* allowed, then VPOP3 will check the **Target Whitelist** and **Target Blacklist** lists to see if the specific recipient is allowed as below. The **Target Whitelist** and **Target Blacklist** can contain individual email addresses or wildcard addresses, eg *@example.com.

1. If both lists are empty, then the recipient is allowed, otherwise:
2. If the blacklist is not empty, and the recipient is contained in the blacklist then the recipient is not allowed, otherwise:
3. If the whitelist is not empty and the recipient is contained in the whitelist then the recipient is allowed, otherwise:
4. The recipient is not allowed.

The **Allow receiving of Internet mail** option lets you indicate whether this user can receive messages from external sources. If you want to restrict a user to only receiving messages from other users on this VPOP3 server, then remove the check from this box. Any remote senders will receive a response from VPOP3 as if the user does not exist. If Internet mail *is* allowed, then VPOP3 will check the **Sender Whitelist** and **Sender Blacklist** lists to see if the specific sender is allowed as below. The **Sender Whitelist** and **Sender Blacklist** can contain individual email addresses or wildcard addresses, eg *@example.com.

1. If both lists are empty, then the sender is allowed, otherwise:
2. If the blacklist is not empty, and the sender is contained in the sender then the recipient is not allowed, otherwise:
3. If the whitelist is not empty and the sender is contained in the whitelist then the sender is allowed, otherwise:
4. The sender is not allowed.

If the **Monitor Messages** box is checked, and the [Message Monitoring](#) options are set to **Selected**, then this user's messages will be monitored as appropriate.

If the **Allow Sending BCCs** box is unchecked, then this user will not be able to send messages including BCCs. Because BCCs are not explicitly specified when sending a message, VPOP3 detects BCCs by comparing the [SMTP envelope](#) recipients with the recipients listed in the To and Cc header

fields. If the SMTP envelope contains recipients not listed in the To or Cc headers, then VPOP3 assumes that a BCC has been used.

Status Monitor Permissions

The Status Monitor Permissions indicate what the user can see and do through the [VPOP3 Status Monitor](#) if they log into it.

- **Allow user to view connection status** - the user can see whether VPOP3 is collecting/sending mail or idle, etc.
- **Allow user to view total queue message counts** - the user can see the total number of messages waiting in users' inboxes.
- **Allow user to view user queue message counts** - the user can see the number of messages waiting in individual users' inboxes.
- **Allow user to view server activity log** - the user can see the details of sending/receiving messages, including who the senders & recipients of messages are.
- **Allow user to initiate connections on server** - the user can tell VPOP3 to start or stop a connection to send and/or collect messages.
- **Allow user to shutdown to the server** - the user can tell VPOP3 to shutdown or restart (obviously, not recommended for non-administrators!)
- **Allow users to receive instant messages** - the user can receive basic instant messages from other VPOP3 users through the status monitor.
- **Allow users to send instant messages** - the user can send instant messages to other VPOP3 users through the status monitor.

5.1.2.7 Aliases

The screenshot shows the 'Edit User - sales' window. At the top right is a 'Submit' button. Below it is a navigation menu with the following tabs: Prune Rules, Folders, Finger Info, Sender Address, Message Rules, Quotas, Address Book, Outgoing Sig, Internal Sig, Advanced, Media, General, Passwords, Routing, WebMail Settings, Autoresponder, Permissions, and Aliases. The 'Aliases' tab is selected. Below the navigation menu are 'New' and 'Delete' buttons. The main area contains a table with the following columns: Email Address, Type, In Mail, and Comments. The table lists several aliases:

Email Address	Type	In Mail	Comments
accounts	Always	All In Main settings	
enquiries	Always	All In Main settings	
faxeval	Always	All In Main settings	
info	Always	All In Main settings	
reseller	Always	All In Main settings	
reseller_sales	Always	All In Main settings	
resellers	Always	All In Main settings	
sales	Always	All In Main settings	

The user's **Aliases** tab defines the aliases/Mappings for the user. These let you explicitly specify email addresses for this user.

This tab simply shows any [Mappings](#) which have this user as the Target.

For help with this tab, you should look at the [Mappings](#) topic. The only difference is that you can't specify the 'Target' when managing Mappings through the Aliases tab because the Target is always this user.

5.1.2.8 Message Rules

Name	Type	All
Delete Junk	In,Local,Sys	<input type="checkbox"/>
Test	In,Local,Sys	<input type="checkbox"/>
Spam false positives	In,Local,Sys	<input checked="" type="checkbox"/>
Domain Name update requests	In,Local,Sys	<input checked="" type="checkbox"/>
Delete Alex junk	In,Local,Sys	<input checked="" type="checkbox"/>
New Rule	In,Local,Sys	<input checked="" type="checkbox"/>
TestForward	In,Local,Sys	<input checked="" type="checkbox"/>

The user's **Message Rules** tab lets you define rules for what happens when messages arrive in this user's Inbox folder ([VPOP3 Enterprise](#) only).

VPOP3 processes Message Rules from top to bottom in the list and a rule can indicate that VPOP3 should stop processing after that rule. You can reorder the rules using the **Move Rule Up** and **Move Rule Down** buttons at the bottom of this page.

Adding or editing a Message Rule

To add a Message Rule, press the **Add Rule** button. To edit a rule, either select it and press the Edit Rule button or simply double-click a rule in the list.

Edit Message Rule

Close Submit

Rule Name :

Conditions [Add](#) [Remove](#)

Field	I	N	Match Type	Data
Subject	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Contains	WARNING from CallServer 192.168.0.30

Actions [Add](#) [Remove](#)

Field	Data
Copy to Folder	Testrule

All conditions need to match

Message Types : incoming Local System

The **Rule Name** is simply a name to help you find it in the future.

Conditions is a list of conditions which must match for the rule to be triggered

Actions is a list of things to do when the rule is triggered

If the **All conditions need to match** box is checked, then all the specified Conditions need to match for the rule to be triggered. If it is not checked, then any one of the conditions is sufficient to make the rule be triggered.

If you have more complicated needs than that, you can have rules check if previous rules matched. For instance, you could have one rule which checks for any one of a number of different subject texts, and then another rule which checks for a specific sender and also that the previous rule was matched.

The **Message Types** boxes let you specify what type of message should be processed by this Message Rule. The options are **Incoming** (from an external sender), **Local** (from a local sender), or **System** (from VPOP3 itself - e.g. error messages).

Conditions

A condition has 5 parts:

- Field/thing to check

- Case insensitive flag - if this is checked then any text comparison is case insensitive. If it is not checked, then comparisons are case sensitive.
- Negation flag - if this is checked, then the condition match condition is inverted
- Match type
- Data to check for

Field

The Field to check for is either an email header field (you can type anything you wish) or one of the offered options. If you want to specify a header field manually, then you can tell VPOP3 to look in multiple fields by separating them with commas, for instance "to,cc" will tell VPOP3 to perform the test in both the to and cc header fields. If either matches then the condition matches.

The pre-defined options are:

- Subject - check the subject header
- To - check the To header
- Cc - check the Cc header
- To or Cc - check both the To and Cc headers
- From - check the From header
- From, To or Cc - check the From, To and Cc headers
- Body - check the message body
- Size - check the message size
- Spam score - check the message spam score (if the VPOP3 spamfilter is enabled)
- Quarantined - check to see if the message is about to be quarantined
- Marked read - check to see if the message is about to be marked read
- Keyword - check to see if the message will have the specified IMAP4 keyword
- Flagged - check to see if the message is about to be marked as 'flagged' (or 'starred')
- Previous Rule Match - check to see if a previous message rule has matched (VPOP3 looks for the rule name)
- Date now - check the date now
- Time now - check the time now
- Message date - check the date the message was sent

Match Type

The **Match Type** indicates how the message data should be compared to the **Data** to check for. For instance, greater than, or contains etc.

Actions

VPOP3 performs all the specified actions. The order is irrelevant.

The available actions are:

- Stop processing after this rule - VPOP3 will perform all the specified actions then not perform any more Message Rule checks.
- Flag Message - the message will be flagged (or 'starred') for an IMAP4 client
- Delete - the message will be deleted
- Quarantine - the message will be quarantined
- Mark Read - the message will be marked as read.
- Add Keyword - add the specified IMAP4 keyword to the message. How this is displayed in your email client will depend on the email client you are using, and how it handles IMAP4 keywords.
- Copy to Folder - copy the message to the specified folder as well as the Inbox (the folder will be created if it does not already exist)
- Move to Folder - move the message to the specified folder instead of the Inbox (the folder will be created if it does not already exist)
- Forward to - forward a copy of the message to the specified email address
- Set Forward sender addr - when forwarding a copy, set the sender address to the specified email address (the same sender address will be used for all forwarded messages due to this rule)
- Modify Headers - use the specified header modifier (eg "MyHeader: blob" will add a header called 'MyHeader' with data 'blob' into the message header). This might be useful for email client filtering later.

5.1.2.9 Outgoing Sig

Signature to be added to outgoing messages

Don't add a signature with messages from this account (requires SMTP authentication)

If these signatures are blank, then VPOP3 will use the Global Signature defined in Settings -> Global Signature. It will only use this signature if the user authenticates when sending outgoing mail.

Signature (Plain text):

Signature (HTML):

The user's **Outgoing Sig** tab defines a signature to be added to outgoing messages sent by this user. For a signature to add to internal messages see the [Internal Sig](#) tab.

Signatures are sometimes also known as *footers* or *disclaimers*, but in VPOP3 they are known as signatures which is a common email term.

VPOP3 lets you configure different signatures for internal and outgoing mail because often signatures for outgoing messages are long and verbose, and there is no need for them when sending internally.

To use personal signatures, your users need to use [SMTP Authentication](#) for sending messages, so that VPOP3 knows which user is sending the message.

If you don't define any user-specific signatures, then VPOP3 will use the global signatures defined in Settings -> [Global Signature](#). If you do define a personal signature, then VPOP3 will use that instead. If you don't want to define a personal signature and don't want to use the global signature then you can check the **Don't add a signature with messages from this account** box.

Please see the [Global Signature](#) topic for more information on the signature content and how it is used.

5.1.2.10 Internal Sig

Submit

Prune Rules	Folders				Finger Info	Sender Address
General	Passwords	Routing	WebMail Settings	Autoresponder	Permissions	Aliases
Message Rules	Quotas	Address Book	Outgoing Sig	Internal Sig	Advanced	Media

Signature to be added to internal messages

Don't add a signature with messages from this account (requires SMTP authentication)

If these signatures are blank, then VPOP3 will use the Global Signature defined in Settings -> Global Signature. It will only use this signature if the user authenticates when sending internal mail.

Signature (Plain text):

Signature (HTML):

Paragraph Font Name Size Bold Italic Underline

The user's **Internal Sig** tab defines a signature to be added to internal messages sent by this user. For a signature to add to outgoing messages see the [Outgoing Sig](#) tab.

Signatures are sometimes also known as *footers* or *disclaimers*, but in VPOP3 they are known as signatures which is a common email term.

VPOP3 lets you configure different signatures for internal and outgoing mail because often signatures for outgoing messages are long and verbose, and there is no need for them when sending internally.

To use personal signatures, your users need to use [SMTP Authentication](#) for sending messages, so that VPOP3 knows which user is sending the message.

If you don't define any user-specific signatures, then VPOP3 will use the global signatures defined in Settings -> [Global Signature](#). If you do define a personal signature, then VPOP3 will use that instead.

If you don't want to define a personal signature and don't want to use the global signature then you can check the **Don't add a signature with messages from this account** box.

Please see the [Global Signature](#) topic for more information on the signature content and how it is used.

5.1.2.11 Advanced

The screenshot shows the 'Edit User - Postmaster' window with the 'Advanced' tab selected. The window title is 'Edit User - Postmaster' and it has a 'Submit' button in the top right corner. The interface is organized into several sections:

- Prune Rules** and **Folders** tabs are visible at the top.
- Change Internet Mail Reply Address to :** A text input field with a help icon.
- Windows Username :** A text input field with a help icon. Below it, the text reads: "Domain\UserName (VPOP3 uses this if 'Allow Windows Passwords' is enabled - if this is left blank, then your VPOP3 username is used as your Windows username)".
- Spam Quarantine Threshold :** A dropdown menu set to 'Global' and a numeric input field set to '100' with a help icon.
- Daily Quarantine Report Recipient :** A text input field with a help icon.
- Store and Fwd email target:** A text input field with a help icon.
- Store and Fwd target server:** A text input field with a help icon.
- Message Recycle Bin Size:** A section showing 'Since' with a date dropdown ('18 Nov') and a time dropdown ('0:00'). Below this, it displays '0 message(s) in existing folders (0 bytes)' and '0 message(s) in 0 deleted folder(s) (0 bytes)(config)'. There is an 'Undelete' button and checkboxes for 'Mark undeleted messages: unread' (checked) and 'starred' (unchecked). A note states: "(The 'mark undeleted messages' options do not apply to folders which are undeleted)".
- Outgoing mail priority:** A numeric input field set to '99' with a help icon and the text "(lower values are higher priority)".
- Hold outgoing messages for:** A numeric input field set to '1', a dropdown menu set to 'Global', and a help icon with the text "(Global is: never)".
- Delete outgoing messages after:** A numeric input field set to '1', a dropdown menu set to 'Global', and a help icon with the text "(Global is: never)".

The user's **Advanced** tab contains some 'advanced' settings for a VPOP3 user.

The **Change Internet Mail Reply Address to** option will change the *From* or *Reply-To* address for any messages sent by this user to the specified email address. This option is rarely needed, because the sender email address is usually set in the email client, but sometimes this can be useful - for instance if you have different internal email addresses from the Internet visible email addresses, or to enforce sender email addresses.

The **Windows Username** setting is only needed if you have [configured VPOP3 to allow users to use Windows passwords](#) to login to VPOP3, and the VPOP3 username does not match the Windows username. You specify this as **Domain\Username** - e.g. **company\fred**

Spamfilter

The **Spam Quarantine Threshold** tells VPOP3 when messages should be quarantined by the VPOP3 [spamfilter](#). The spamfilter gives each incoming message a 'spam score', with 'spammier' messages

having a higher score. The default is that if the score is 100 or more, then messages will be quarantined, but you can change this for individual users who may want to receive less spam (with more risk of false positives) or have less chance of false positives (so possibly receive more spam). You can **disable** the quarantine for this user, use the [Global quarantine threshold](#), or set it to a **custom** value.

The **Daily Quarantine Report Recipient** specifies the email address which will receive the report listing messages quarantined by the spamfilter for this user. If this is left blank, then the quarantine report will go to the address specified in the global settings. If that is also blank, then the quarantine report will go to this user.

Store and Forward Settings



VPOP3 Enterprise

The following option is only available in the [Enterprise edition](#) of VPOP3.

Store and forward is an advanced option where VPOP3 will put a message into the user's Inbox folder, and at the same time attempt to forward it to another mail server using SMTP.

This is different from normal LAN Forwarding because the messages are copied to both the user's Inbox *and* to the other mail server. VPOP3 will then keep the messages in sync, so if the message is deleted from the Inbox folder, it won't forward it to the other mail server, and if the message is forwarded to the other mail server, it will delete it from the Inbox folder.

The purpose of this facility is for it to be used as a backup service. For instance, if you have set up this installation of VPOP3 as a secondary MX server, then while the primary server is working, messages will be forwarded onto the primary server, and the local Inboxes won't fill up, but then if the primary server fails, users can access their new messages via this server without any reconfiguration. If and when the primary server recovers, then messages will start flowing to that server again.

The **Store and Fwd email target** setting specifies the email address for the messages to be forwarded to.

The **Store and Fwd target server** setting specifies where the messages should be forwarded to. This can be a simple IP address or host name, or you can add alternate ports and authentication details. The full syntax is:

```
[username:password@]hostname[:port]
```

For instance, valid entries could be:

- 192.168.10.2
- mailserver.mycompany.com:25
- fred:bibble@mailserver.mycompany.com:587

VPOP3 will use *STARTTLS* encryption if the remote server supports it, but will not use SSL encryption.

Recycle Bin



VPOP3 Enterprise

The following option is only available in the [Enterprise edition](#) of VPOP3.

VPOP3 Enterprise has a **Recycle Bin** option, where messages & folders which are deleted by the user will be retained in the message store in a 'zombie' state for a few days. These messages can then be undeleted by an administrator if the user realises they didn't mean to delete the messages.

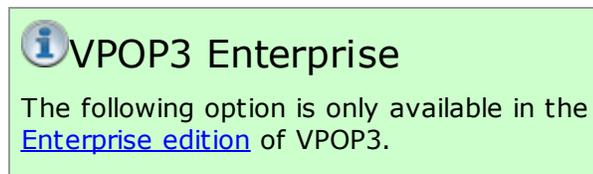
The recycle bin is configured in the [Database settings](#). In the user's settings you can undelete the messages.

You select the time just before the desired messages were deleted in the date & time boxes after the **Since** text. Once you have chosen a date/time, you will be told how many messages & folders were deleted after that time.

You can also tell VPOP3 to mark the recovered messages in existing folders as *unread* and/or as *starred/flagged*. This will make it easier to find the recovered messages and deal with them.

Once you are ready, press the **Undelete** button to recover the messages.

Outgoing Mail handling



You can tell VPOP3 how to treat outgoing messages sent by this user (these settings do not apply to internal messages sent by the user). If you wish to use these settings, then you should make sure that you [require SMTP authentication](#) when sending messages, so that VPOP3 knows which user has sent which messages.

These settings can be set on a user basis. A Lua script can override these settings if desired.

The **Outgoing mail priority** lets you prioritise some users' messages over others (lower numbers are higher priority - e.g. messages with priority 1 are sent before those with priority 2). If messages fail and are retried, VPOP3 will adjust the priority so that they move back in the priority list to avoid blocking newly sent messages.

The **Hold outgoing messages for...** setting lets you tell VPOP3 to hold outgoing messages in the [Outqueue](#) for a time after they are sent. This can be useful, for instance, if you want to approve some users' emails before they are sent, or if some senders like a 'grace period' after they have sent their messages so that messages can be deleted in case they change their minds. The default value is set in the [Misc Settings](#), but it can be overridden for each user if desired.

The **Delete outgoing messages after...** setting lets you tell VPOP3 to delete a users' messages from the Outqueue if they have not been sent for a certain amount of time. The default value is set in the [Misc Settings](#), but it can be overridden for each user if desired. A related setting is set in the [Mail Sender settings](#) as the **Max Retry Time**, but that only applies when the **Mail Sender** tries and fails to send the message. This setting will apply even if the message is **Held**, or no **Mail Sender** tries to send it. If a message is deleted because of this setting, the sender will receive notification that this has happened.

You could, for instance, set the **Hold outgoing messages for...** to 2 days, and the **Delete outgoing messages after** to 1 day. Then, the message will be deleted before it is automatically unheld, so an administrator needs to unhold the users' messages within the first day after they are sent for them to go, otherwise they will be deleted automatically, and the sender notified.

5.1.2.12 Prune Rules

Folder	Age	Size	Read	Flagged	Deleted	Spam
Archive	365		Either	Either	<input type="checkbox"/>	<input type="checkbox"/>



VPOP3 Enterprise

The following option is only available in the [Enterprise edition](#) of VPOP3.

A user's Prune Rules tell VPOP3 to automatically delete a user's messages based on certain rules.

If the **Use global Prune Rules** box is checked, then you cannot configure user-specific prune rules. Instead the user uses the default prune rules defined in Settings -> [Database](#) -> [Message Store](#).

If the **Use global Prune Rules** box is not checked, then you can configure user-specific rules instead.

To add a rule, press the **Add Rule** button. To remove one, select it, then press the **Delete Rule** button.

- The **Folder** column indicates the folder for the rule to act on. Use * to mean all folders
- The **Age** column indicates the age of messages which should be deleted - eg 365 will delete messages over 365 days old.
- The **Size** column indicates the size of messages which should be deleted (blank means any size)
- The **Read** column indicates whether read messages should be deleted (can be set to Read, Unread or Either)
- The **Flagged** column indicates whether flagged (starred) messages should be deleted (can be set to Flagged, Unflagged or Either)

- The Deleted column indicates whether only IMAP4 deleted messages should be (really) deleted, or all messages. If this is checked, the prune rule will *only* delete messages which have been marked as IMAP4 deleted.
- The Spam column indicates whether only messages which VPOP3 detected as spam should be deleted, or all messages. If this is checked, the prune rule will *only* delete messages which VPOP3 detected as spam.

All conditions must match for a message to be deleted. Deleted messages are put into the Message Recycle Bin so can be undeleted if you get the Prune Rule wrong and discover it in time.

For instance, you could set:

- Folder = *
- Age = 30
- Size = <blank>
- Read = Either
- Flagged = Either
- Deleted = checked
- Spam = unchecked

This will really delete (IMAP 'purge') all messages which have been marked as deleted in an IMAP client after 30 days. This can be useful if you have an email client such as older versions of Microsoft Outlook which does not handle IMAP4 deleted messages very well.

A common problem is due to people leaving the **Deleted** and **Spam** checkboxes checked. When adding a new rule, VPOP3 checks these boxes for the new rule to make it unlikely to delete any wanted messages, but if you leave the boxes checked, then VPOP3 will *only* delete messages which were both marked as spam by the spamfilter, and messages which have been marked as IMAP4 deleted already. It will not delete messages which the user has not marked for deletion.

5.1.2.13 Folders

Name	Messages	Unread	Size	Owner Perms
<input type="checkbox"/> Inbox	8223	8118	350.7MB	lrswiploteacd
<input type="checkbox"/> Deleted Items	0	0	0	lrswiploteacd
<input type="checkbox"/> Drafts	0	0	0	lrswiploteacd
<input type="checkbox"/> Sent Items	0	0	0	lrswiploteacd

Select All/None Empty Selected Delete Selected Export EML Export MBOX 0 folder(s) selected.

Copy/move to user 1calldirect Move Copy

Rename folder to Rename

Set folder owner permissions to Full permissions Set

The user's **Folders** tab lets the administrator manage a user's mail folders. This is only available in [VPOP3 Enterprise](#).

The main section of the page shows the folders for the user in a tree structure. You can select folders by clicking on them or ctrl-clicking or shift-clicking them to select multiple folders. If a folder with subfolders is 'collapsed' (so only the parent folder is visible) then selecting that folder will also select subfolders. The **X folder(s) selected** text under the folder list indicates how many folders are currently selected.

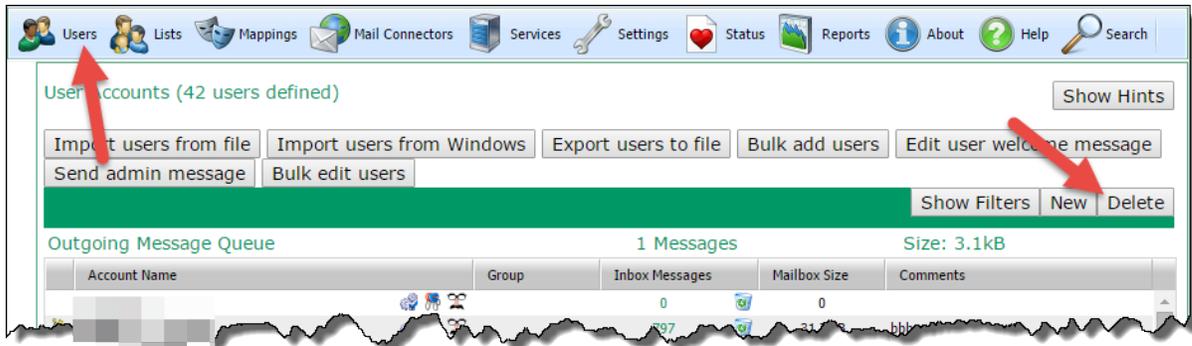
Once you have selected folders, you can perform actions on them:

- **Empty Selected** - this action will delete all messages from the selected folders. If necessary you can undelete messages using the [recycle bin function](#).
- **Delete Selected** - this action will delete the selected folders (and the messages in them). If necessary you can undelete messages using the recycle bin function.
- **Export EML** - this action will create a ZIP file containing [EML files](#) (one per message) from the selected folder(s) and then download it to the operator's computer.
- **Export MBOX** - this action will create a ZIP file containing [MBOX files](#) (one per selected folder) and then download it to the operator's computer.
- **Move/Copy** - these actions will move or copy the selected folders to the specified user.
- **Rename folder to** - this action will rename the specified folder (can only be used if only one folder is selected).

- **Set folder owner permissions to** - this lets you specify that the owner has full permissions to the folders, or that the user cannot rename/move or delete the selected folders.

5.1.3 Deleting a User

To delete a user, go to the **Users** page in the VPOP3 settings, select the user(s) you wish to delete, and press the **Delete** button.



When you delete a user, then this will delete any [Mappings](#) or [list memberships](#) associated with that user. Any administrative features, such as [Main Administrator](#) setting, or [Message Targets](#) will be redirected to the Main Administrator, or the currently logged in user if the Main Administrator is being deleted.

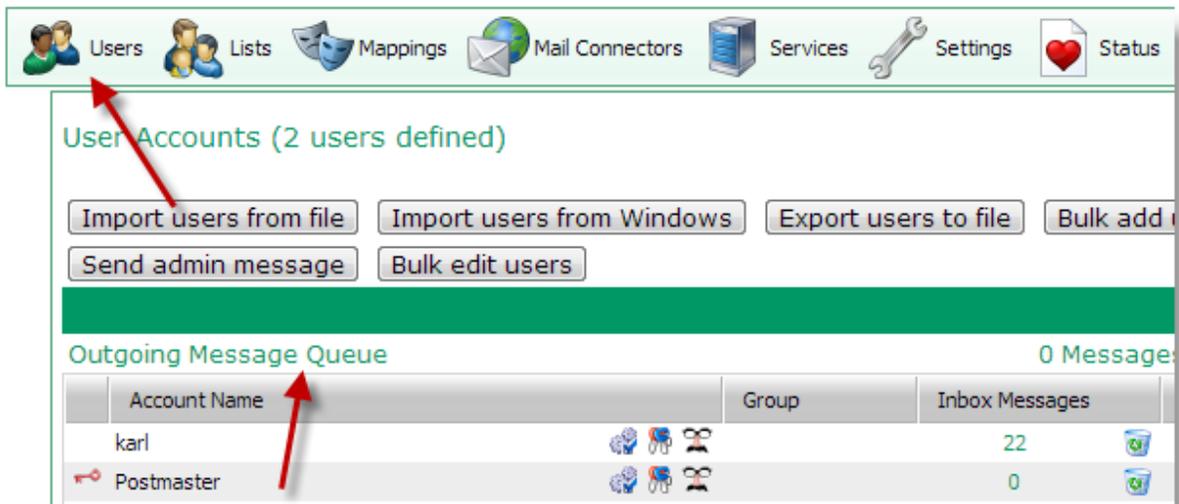
You cannot delete the currently logged in administrator. If you wish to delete that user, you need to edit another user and set them to be an administrator, then log out of the VPOP3 settings, and log back in as that user, then delete the original user.

You cannot delete a user who is currently logged into VPOP3 in any way (eg in an email client). VPOP3 will say that the user is "in use" in that case, and you need to have them log out. Note that this can also happen if the VPOP3 Status Monitor is logged in as that user. You can go to [Status](#) -> Sessions, to see if the user is logged in, and from which IP address(es) and using which protocols.

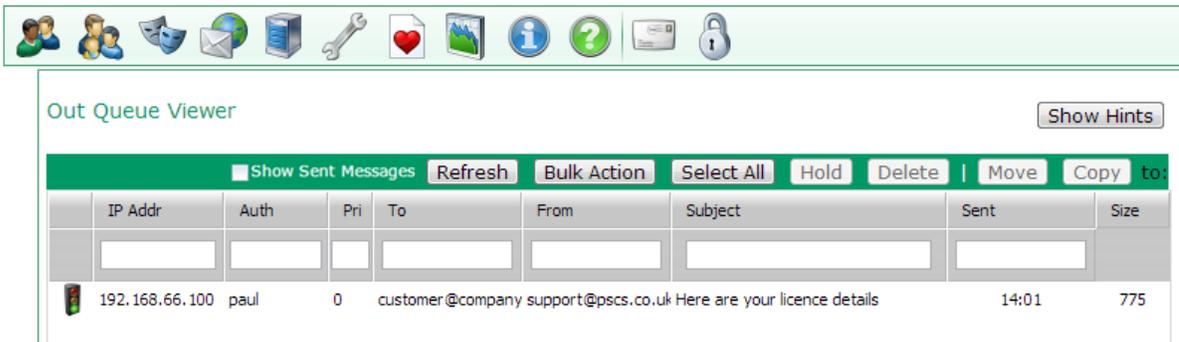
When you delete a user who has messages in their mailbox, then VPOP3 will warn you and ask you to confirm that you wish to empty that user's mailbox before deleting the user. If you wish to save the user's messages then you should copy the messages *before* you delete the user. You cannot recover the user's messages after you have deleted the user. Note that a user may have messages in their mailbox which are not in their Inbox folder, so VPOP3 may warn you about messages being in the user's mailbox, even if the **Inbox Messages** column shows zero messages for that user.

5.1.4 Manage outgoing message queue

The VPOP3 Outqueue is where VPOP3 stores messages waiting to be sent out to remote users.



To access the VPOP3 Outqueue, click the Users button at the top of the screen, then click on some text in the **Outgoing Message Queue** line just above the list of users.



The Outqueue viewer shows all the messages waiting to be sent out by VPOP3.

Grid columns

In the table the columns show details of the message:

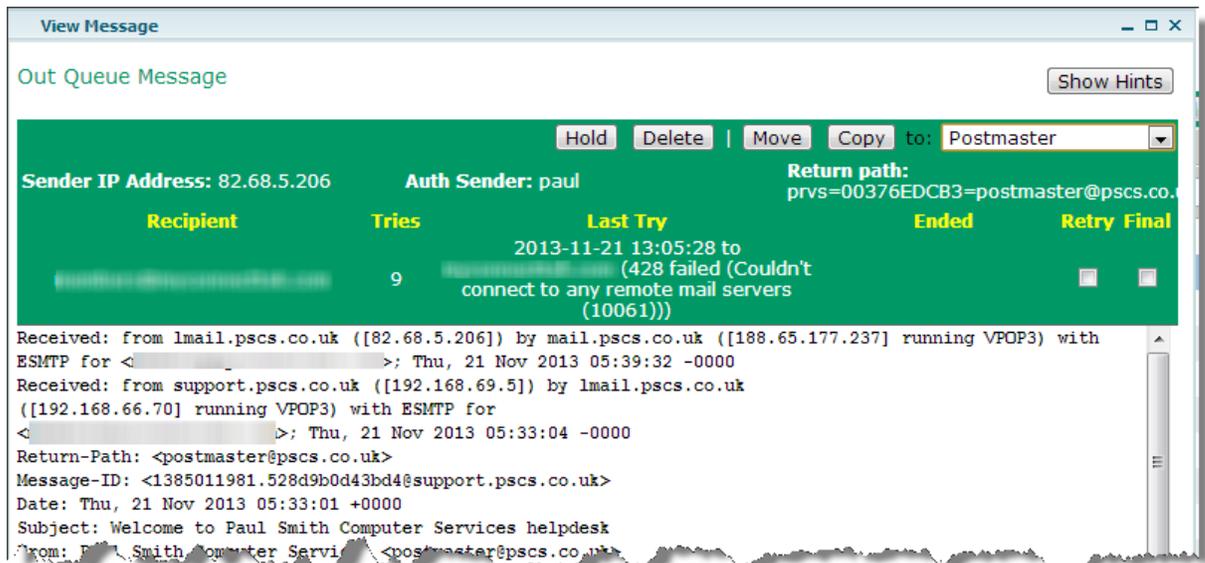
- **State** - the left hand column shows the 'state' of the message. This is one of: held (), held on a timer (), not held (), or currently being sent (). VPOP3 will not send messages which are currently held. In a [user's Advanced settings](#) you can tell VPOP3 to hold a user's sent messages for a short time before letting them be sent. An administrator can manually hold/unhold messages.
- **IP Addr** - the IP address which the message was sent from. If the message was sent by VPOP3 itself, this will show 'unknown'.
- **Auth** - the authenticated user who sent the message. This will be blank if the sender did not use SMTP authentication when sending the message.

- **Pri** - this is the 'priority' of the message. VPOP3 will send messages with a smaller priority number first. The priority can be set on all of a user's emails in the [user's Advanced settings](#). Also, a Lua script can alter the priority of emails as they arrive at VPOP3.
- **To** - this is who the message is addressed to (this shows the SMTP envelope recipients which may not be the same as the message header displays)
- **From** - this shows the SMTP return path address (which may not be the same as the From address in the message header)
- **Subject** - this shows the message subject
- **Sent** - this shows when the message arrived at VPOP3
- **Size** - this shows the message size

Using the grid

- ❖ You can filter the messages displayed by [typing into the filter boxes](#) under the column headers.
- ❖ You can select messages by clicking on them in the message list. You can use shift-click or ctrl-click to select multiple messages.
- ❖ You can refresh the Outqueue message list by clicking the **Refresh** button.
- ❖ You can perform [bulk actions](#) on many Outqueue messages at once by pressing the **Bulk Action** button.
- ❖ You can select all the displayed messages by clicking the **Select All** button.
- ❖ You can hold or unhold the selected messages by clicking the **Hold/Unhold** button. Held messages are not sent by VPOP3.
- ❖ You can delete the selected messages by clicking the **Delete** button.
- ❖ You can move or copy the selected messages to a user's Inbox mail folder by selecting the user from the drop-down list and pressing the **Move** or **Copy** buttons.
- ❖ If you check the **Show Sent Messages** box, then VPOP3 will display recent messages which it has successfully sent out, or which have failed. By default this holds the last 3 days' worth of messages.

Viewing a message



If you double-click on a message in the list, you will be able to see the message contents, and some more details about the message.

You can **Hold**, **Delete**, **Move** or **Copy** the message from the view window just as from the main message list.

This window also displays the sender IP address, authenticated sender, SMTP Return path, recipient(s) as on the message list.

In addition, it shows how many times VPOP3 has tried to send it, what the result of the last attempt to send the message was, when the message was sent successfully (currently always blank).

There are also two checkboxes:

- **Retry** - this tells VPOP3 to try sending the message the next time it sends messages, even if the [Sender Retry rules](#) would tell VPOP3 not to try sending the message again for a while.
- **Final** - this tells VPOP3 that the next retry should be the last. If the next retry does not succeed, VPOP3 will fail the message as if it had [run out of time for retrying](#).

If you change the values of **Retry** or **Final**, it takes effect immediately.

5.1.4.1 Bulk Actions

You can perform bulk operations on messages in the [VPOP3 Outqueue](#) here. To get to this page, go to [Users](#), click on the **Outgoing Message Queue** at the top of the table of users, then click on **Bulk Action**

Outqueue Mass Action

Close

Action to perform: Force Retry ▾

Search Criteria

Size between: 0 and 999999 kB

Subject:

Source IP:

Auth Sender:

To:

From:

Held Messages

Messages Affected: 0

Refresh Affected Message Count Process Action

You can use * and ? wildcards in the text boxes, or use regular expressions surrounded by '/' characters - eg /Price: [0-9]{3}\.[0-9]{2}/i

Leave text boxes blank to match any text for that data.

Outqueue Bulk Action

You can perform four different actions on the chosen messages:

- **Force Retry** - this will tell VPOP3 to retry sending the messages the next time it connects to send messages. Normally VPOP3 will wait between retries depending on rules configured in the [Mail Sender](#), this option will override that delay. Note that VPOP3 will only retry sending the message to any recipients who have not accepted the message or rejected the message permanently.
- **Delete** - this will delete the messages from the Outqueue
- **Hold** - this will mark the messages as held. That means that the messages will still stay in the Outqueue, but VPOP3 will not attempt to send them. You may unhold the messages later either individually on the main Outqueue page, or through further bulk actions.
- **Unhold** - this will remove the hold marker from the messages, so VPOP3 will attempt to send the message as normal

The main section of the page lets you specify which messages will be acted upon

- **Size between** - lets you specify the size of the message to be processed
- **Subject** - lets you specify text in the subject to search for
- **Source IP** - lets you specify the IP address the message should have come from
- **Auth Sender** - lets you specify the authenticated user who sent the message

- **To** - lets you specify the email address of a recipient the message was for
- **From** - lets you specify the email address of the sender
- **Hold** - if this is checked, then only held messages will be processed (if they match the other conditions). If not checked, then only unheld messages will be processed.

Subject, Source IP, Auth Sender, To, and From are usually case insensitive substring matches, but you can specify a regular expression match by surrounding the text with `/.../` characters (make it case insensitive by appending `i` after the final `/`. If you leave any of these boxes empty, then that field will not be checked. For instance:

- **invoice** - will match anything containing Invoice, invoice, iNvOiCe, etc
- **/invoice/** - will match anything containing invoice, but not Invoice etc
- **/^invoice/** - will match anything beginning with invoice
- **/^invoice\$/** - will only match invoice exactly
- **/^invoice/i** - will match anything beginning with invoice, Invoice, iNvOiCe, etc

The **Messages Affected** count will tell you how many messages will be affected by the current conditions at this moment.

The **Refresh Affected Message Count** button will tell VPOP3 to recalculate how many messages will be affected. This may be useful if more messages are arriving or being sent, or the conditions are changed.

The **Process Action** button will tell VPOP3 to process the selected action on the chosen messages. This will report the number of items affected after the action is complete. Note that this count may be different from the **Messages Affected** count because more messages may have arrived since that was calculated. Also, note that for the **Force Retry** action, the result count shows the number of target recipients affected, not the number of messages, so if messages are sent to more than one recipient who needed retrying, the resulting count may be larger than expected.

5.1.5 Import users from file

The **Import users from file** button will let you load a list of users from a CSV file. Some people have used this for copying users from one installation of VPOP3 to another, but that is not recommended in most situations because the **Export** and **Import** facilities only handle a very small proportion of user settings so it is likely that the user configuration you have after the import on the new installation will not be the same as it was on the old installation.

If you want to copy a VPOP3 installation to a new PC, then see the Move VPOP3 instructions.

Generally the **Export** and **Import** facilities are useful if you want to manage users in a spreadsheet program or get a list of users for use elsewhere or something similar. For instance you could export a list of users, then add some new users or change a forwarding address or something, and then re-import them back. This will keep all the existing settings except for the changes and will add the new users. This is different from expecting it to make a full copy of your user configurations.

The **Import** can also be useful when initially setting up a new VPOP3 installation with a large number of users, but the [Bulk Add Users](#) facility may be easier in many cases.

To import the users from a file go to the [Users](#) page and press the **Import users from file** button on the top row. A window like that below will appear:

Import Users From File

[Help](#) [Show Hints](#)

[Close](#) [Preview Import](#)

You should select a suitable CSV (Comma Separated Variables) file to be used to merge with or replace the existing user database.

File to import : No file chosen

You will be able to set further settings on the next page before the file is actually imported. This includes associating the CSV file columns with the VPOP3 user data fields.

Possible data columns which can be imported into VPOP3

- User Id
- Password and Webmail Password
- Administrator flag (1/0)
- Forward To email address(es) and "Use Forwarding" flag (1/0)
- Assistant email address(es) and "Send only to assistant" flag (1/0)
- Comments
- Internet reply address
- "In 'Everyone' list" flag (1/0)
- "Is allowed to send Internet mail" flag (1/0)
- "Is allowed to receive Internet mail" flag (1/0)
- Should messages be monitored flag (1/0)
- Maximum outgoing message size (in bytes)
- Template user (see help)
- Other options (see help)

VPOP3 will import the data from a CSV (Comma Separated Variables) file which most spreadsheet programs will be able to load. Often the best thing to do is to use the [Export users to file](#) option to create a sample CSV file, then edit that in your spreadsheet program and import the edited CSV file. Make sure you tell the spreadsheet program to save it as a CSV file. VPOP3 will not be able to read an XLS or similar file.

Select the file by pressing the **Choose File** button next to **File to import**, and then press the **Preview Import** button. VPOP3 will not import the users at this point, and you will be given the opportunity to confirm or cancel the operation.

After pressing Preview Import, VPOP3 will read the first few lines of the file and display a window letting you specify how the file is to be loaded.

Import Users From File ""

Close **Changes have been made - press:** Import File

Import Preview (first 5 lines of file)

In the table below please select which columns of the source file are to be mapped to which VPOP3 user attributes. If you want VPOP3 to ignore the column choose **Ignore**.

User Id	Admin	Password
User Id	Admin	Password
Answermachine	0	LNJJPV
bradley	0	OKNJCPARGUHIKT
cti	1	OLMLDUASGHAJFRLP
elephant	0	LNJJPVNR

Ignore first line
 Update Existing Users
 Remove users not present in imported file

How are passwords to be created?

Encrypted (Using the encryption which VPOP3 uses when exporting to a file)
 From File
 Randomly
 Use the Username
 Use the text "Password"

The top part of the window shows the first few lines split into columns and which user attribute will be associated with which column. You can scroll right to change the attribute -> column assignment if necessary. You can choose **Ignore** in the attribute selector if you want VPOP3 to ignore a specific column.

Below that are options about how VPOP3 will load the data from the file.

- **Ignore first line** - VPOP3 will ignore the first line (which may contain column headers).
- **Update existing users** - VPOP3 will update the settings for any existing users. If this option is not selected, then existing users will not be modified by the import action.
- **Remove users not present in imported file** - VPOP3 will delete any users who are not in the imported CSV file. If this option is not selected, then no users will be deleted.

The **How are passwords to be created** options let you specify how passwords will be set for added/updated users

- **From File** - the password from the file will be used. If **Encrypted** is checked, then VPOP3 will decrypt the password using the same encryption method as used when [exporting the file](#).

- **Randomly** - the password will be set randomly. The administrator can either reset these after the import, or you can read the generated passwords from the *importusers.log* file which is created in the VPOP3 installation directory.
- **Use the Username** - the password will be set to the same as the user name. Please change the password as soon as possible!
- **Use the text "password"** - the password will be set to "password". Please change the password as soon as possible!

Press the **Import File** button to import the file, or the **Close** button to cancel the import operation.

5.1.6 Import users from Windows

The **Import users from Windows** button will let you load a list of users from the Windows users list, such as the Domain Users list.

To import the users from Windows go to the [Users](#) page and press the **Import users from Windows** button on the top row. A window like that below will appear:

Import User Database from Windows User Database

Use this page to import users from the Windows user database into the VPOP3 user database settings.

- Make Windows Administrators into VPOP3 Administrators**
- Modify existing VPOP3 users**
- Send Welcome Message to new users**
- Remove users not present in Windows user database**
- Import 'Guest' accounts**

Windows Group to Import:

VPOP3 will import users from the Windows accounts.

VPOP3 will import the user name, comment, real name, and optionally administrator status.

The **Make Windows Administrators into VPOP3 Administrators** option tells VPOP3 that any VPOP3 users it creates or modifies for Windows users who are administrators should be made into VPOP3 administrators as well.

The **Modify existing VPOP3 users** option tells VPOP3 to update comment, real name & optionally administrator status for existing users who are also Windows users.

The **Send Welcome Message to new users** option tells VPOP3 to send the "welcome message" to any new users.

The **Remove users not present in Windows user database** option tells VPOP3 to remove any VPOP3 users who are in the Windows group being imported. The currently logged in user will not be deleted even if they are not a Windows user.

The **Import Guest accounts** option tells VPOP3 to import any users which are designated as 'guest' accounts in Windows. This should usually be turned off.

The **Windows Group to Import** option tells VPOP3 which users it should import. You could create a Windows group specifically for email users, or use a standard one such as *Domain Users* or similar. VPOP3 will import any users who are members of the specified group.

Press the **Import File** button to import the users, or the **Close** button to cancel the import operation.

VPOP3 will remember the settings on this page, so if you perform the action again later, the previous settings will be set as the new defaults to make it easier to import the same Windows group again, and so on.

VPOP3 cannot import passwords from Windows, because Windows does not allow access to stored passwords. Instead, newly created users will be given a password of 'password'. You should reset these at the earliest opportunity.

You can use the **Allow users to log in using their Windows passwords** option in the [Security Settings](#) to allow users to log in using their Windows passwords. In this case VPOP3 will ask Windows if the supplied password is correct, which Windows does allow.

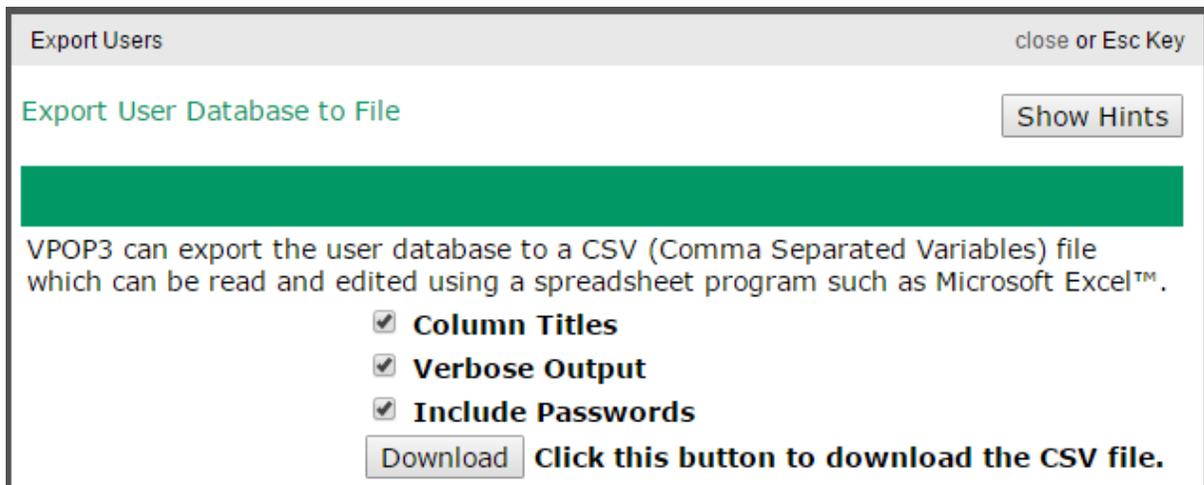
5.1.7 Export users to file

The **Export users to file** button will let you save a list of users to a CSV file. Some people have used this for copying users from one installation of VPOP3 to another, but that is not recommended in most situations because the **Export** and **Import** facilities only handle a very small proportion of user settings so it is likely that the user configuration you have after the import on the new installation will not be the same as it was on the old installation.

If you want to copy a VPOP3 installation to a new PC, then see the Move VPOP3 instructions.

Generally the **Export** and **Import** facilities are useful if you want to manage users in a spreadsheet program or get a list of users for use elsewhere or something similar. For instance you could export a list of users, then add some new users or change a forwarding address or something, and then re-import them back. This will keep all the existing settings except for the changes and will add the new users. This is different from expecting it to make a full copy of your user configurations.

To export the users to a file go to the [Users](#) page and press the **Export users to file** button on the top row. A window like that below will appear:



VPOP3 will export the data to a CSV (Comma Separated Variables) file which most spreadsheet programs will be able to load.

After choosing the appropriate options, press the **Download** button to download the CSV file (as *userlist.csv*).

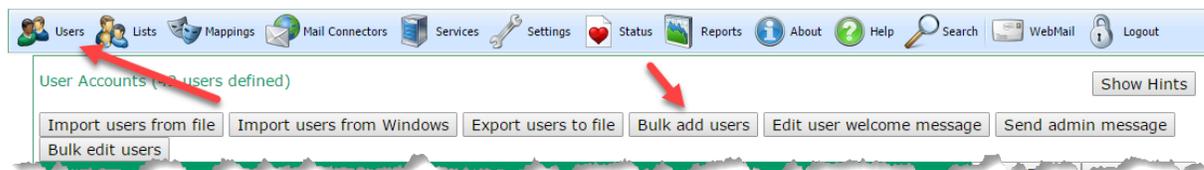
The options available are:

- **Column Titles** - the CSV file will include a title for each column in the table (eg *User Id, Assistant* etc)
- **Verbose Output** - if this is checked, then the CSV file will include all available columns. If it is not checked then the CSV file will only contain the user ids, admin state and possible passwords
- **Include Passwords** - if this is checked, then the CSV file will include encrypted versions of the passwords. If it is not checked, then it won't.

For security reasons, the downloaded CSV file cannot contain plain text passwords. If you ask it to include passwords, then the passwords will be encrypted in the file. The [Import](#) option will handle these appropriately during import.

5.1.8 Bulk add users

If you need to add lots of users to VPOP3 then the **Bulk Add Users** button from the [Users](#) list could be very helpful.



This takes you to a simple form where you can create up to 10 new users just by entering the usernames and passwords.

Bulk Add Users Help Show Hints

Close Submit

	User Name	Password
1	<input type="text"/>	<input type="password"/>
2	<input type="text"/>	<input type="password"/>
3	<input type="text"/>	<input type="password"/>
4	<input type="text"/>	<input type="password"/>
5	<input type="text"/>	<input type="password"/>
6	<input type="text"/>	<input type="password"/>
7	<input type="text"/>	<input type="password"/>
8	<input type="text"/>	<input type="password"/>
9	<input type="text"/>	<input type="password"/>
10	<input type="text"/>	<input type="password"/>

If you set the username as the part of the user's email address which comes before the @ symbol, then in many cases this will be all you need to do to create the user(s).

5.1.9 Edit user welcome message

To get to this page, go to Users -> Edit user welcome message.

Edit Custom Welcome Message Show Hints

Close **Changes have been made - press:** Submit

Welcome Message: Welcome to our email system

In your email client use the following settings to access your account:

Server: mail.example.com
Username: {username}
Password: {password}

If you have any problems contact support@example.com

If you add a line that contains the text "**<Subject: some text>**" then the subject of the welcome message will be "some text", otherwise it will be "Welcome to email".

You can also include the elements "**{username}**" or "**{password}**" to include the specific username or password of the new user if you wish.

Any other text will be sent to the user as it is entered here. (Note that you can only send a plain text message, you cannot use HTML or other formatting characters).

This page lets you configure a welcome message to be sent to new users. When you add a new user, by default this message will be delivered to their VPOP3 mailbox, but you can tell VPOP3 not to send it when you are [adding the user](#).

The message is a plain text message which can contain any content you want. If the message text is blank, then no welcome message is sent, even if it is selected when adding a user.

The message text can contain **{username}** or **{password}** which will be replaced by the new user's username or password respectively.

By default the message will have the subject "Welcome to email", but you can change this by adding a line to the message containing text like

<Subject: some text>

this will replace the message subject to 'some text'. This line will not be included in the message itself when it is sent to the user.

5.1.10 Send admin message

The Send Admin Message button on the Users page lets the administrator send an email message to users

Send Admin Message

Use this page to send an administrative message to a group of VPOP3 users.

Changes have been made - press:

Target Group/List : (n.b. The message will only be sent to local users of the selected list, not remote email addresses!)

Save message for future use

Message Subject :

Message Text :

You can use certain special keywords in the message which will be replaced when the message is sent:

- {username} - will be replaced with the relevant VPOP3 username
- {ldap_...} - will be replaced with the relevant LDAP attribute
- {messagecount} - will be replaced with the number of messages for this user
- {mailboxsize} - will be replaced with the mailbox size for this user
- {mailboxquota} - will be replaced with the mailbox quota for this user
- {lua}...{/lua} - will execute a Lua script - see [the manual](#) for more details

Message Preview

Subject : Message from your Mail Administrator

text : This is a test message to you, paul

VPOP3 Enterprise 7.0 - lmail.pscs.co.uk - 192.168.66.23 | Idle | In: 41294 | Out: 0

This option lets you send bulk messages to your users with the specified text.

The **Target Group/List** setting lets you choose who the message will go to. This is a [Group or Distribution List](#) defined in VPOP3. (You cannot send messages to individual users this way - unless they are the sole member of a list. You can use normal email for that.). The **Everyone** group usually contains all your users if you want to send a message to everyone.

The **Save message for future use** option tells VPOP3 to remember the message you send so that it will appear as the default message the next time you come to this page.

The **Message Subject** box lets you specify the subject of the email you want to send

The **Message Text** box lets you specify the text of the email you want to send. (Note that Admin Messages can only contain text, not HTML).

The **Preview** button lets you view a preview of the message as it would be delivered to yourself.

Text replacements

The **Message Subject** and **Message Text** can contain text replacements to customise the message for the user. These are indicated on the page in the VPOP3 settings

- **{username}** - is replaced by the VPOP3 user name of the recipient.
- **{ldap_xxxx}** - is replaced by the LDAP attribute represented by xxxx for the VPOP3 recipient. For instance {ldap_o} will be replaced by the Company name from their address book entry (the LDAP 'o' attribute for the inetOrgPerson LDAP class contains the 'organisation' for that object).
- **{messagecount}** - is replaced by the number of messages in that user's Inbox.
- **{mailboxsize}** - is replaced by the size of that user's whole mailbox.
- **{mailboxquota}** - is replaced by the mailbox size quota for that user.
- **{lua}...{/lua}** - executes a Lua script (see below) and is replaced by the 'print' output of that script.

Using Lua

One of the options of this facility lets you specify a [Lua](#) script in the message to send. This script lets you customise the message for each user.

See the [Lua scripting topic](#) for details on the VPOP3 Lua implementation.

When a Lua script in the administrator message is run, it has certain global variables set:

- **Username** - contains the username of the user currently being processed
- **MessageCount** - contains the number of messages in the user's inbox
- **MailboxSize** - contains the size of the user's whole mailbox (in bytes)
- **MailboxQuota** - contains the user's mailbox quota setting (in bytes - 0 means no limit)
- **LDAP** - this is a table containing the LDAP attributes for this user - the attribute names are in upper case - eg **LDAP.CN** is the user's 'display name'

(The variable names are case sensitive)

Anything that the script 'prints' gets sent to the user

An example Lua script used in the message sending facility might be

```
{lua}
if MailboxQuota ~= 0 then
  print ("You are currently using " .. MailboxSize .. " bytes of your allowed " .. MailboxQuota
end
{/lua}
```

If the Lua script sets the global variable '**DontSend**' (case sensitive) to '1' then VPOP3 won't send the message to this particular user.

5.1.11 Bulk edit users

If you need to change the settings for several users, then the **Bulk Edit Users** option may be able to help. To get to this page go to To get to this page, to to Users → Bulk Edit Users.

The large box (containing Bob, Kate, Mark, etc in this example) contains a list of all your users. The changes you specify on this page will apply to all the selected users. Selected users are displayed with a dark green background, and the number of selected users is displayed next to the Add/Remove buttons.

You can select or deselect users by clicking on them. Also, you can use the search boxes above this area to search for users by various criteria (wildcards can be used) - so, for instance, searching for Name matching * will find all the users. When you have done a search, matching users will be displayed with a pink background. You can press the Add or Remove buttons to add or remove these users from the Selected list. So, for instance, you could add all the users except those in the 'retired' group by doing the following steps

1. Search for Name matching "*" - press Add, then
2. Search for Group matching "retired" - press Remove

When you have the list of users you wish to modify, you can use the **Changes to make** section to specify what to change. In general, enter the new value in the right-hand column either by typing the new entry, or checking the checkbox as appropriate. Then, make sure the **Set** checkbox in that row is checked, and press the **Submit** button at the top of the page. VPOP3 will apply your changes to the selected users, and they will be marked with a tick when they have had the change applied.

Assistants & Forwards

Starting in v6.15 the Assistant and Forward setting can be modified through this page, rather than just set. This is done by putting + or - at the start of the new value to add or remove values respectively.

So, for instance, you could add a forward to boss@mycompany.com by specifying "+boss@mycompany.com" in the Forward new value. VPOP3 will then add this forward to the existing forwards for the selected users. Similarly to remove a forward, you can put a '-' at the start of the new value. Adding a value which already exists or removing a value which does not exist will not cause any problems.

If you don't specify a + or - at the start of the new value, then the new value will overwrite any existing value.

Quarantine Threshold

If you set the Quarantine Threshold to '-1' it indicates that the quarantine is disabled for those users.

If you set it to '0', it uses the default quarantine threshold set in the [Spamfilter settings](#).

If you set it to any other value, then that value is used for the quarantine threshold.

Custom Setting

The Custom Setting section at the bottom of the page should not be used unless you have been told how to by Technical Support or a VPOP3 support document. This allows you to make changes to certain other settings, but may need special (not obvious) values to do what you want.

5.2 Lists

5.2.1 Using Lists

A list will contain zero or more 'members' (usually email addresses) which can be messaged all at once. To send a message to all the members of a list, you will usually send an email to the listname at a valid domain.

For instance, if your 'Local Domains' setting is set to *mycompany.com;mycompany.org*, and your list is called *Customers*, then you can send a message to all your customers by sending an email to *customers@mycompany.com* or customers@mycompany.org

If you want the list to be accessible using other email addresses, then you can use [mappings](#) to create aliases for the list.

Public Lists

By default, lists can only be accessed internally. Any incoming messages to the list's email address will be treated the same as incoming messages to an unrecognised address.

If you want a list to be accessed from outside your network, you have two options:

- You can tick the **Allow incoming mail to be sent to the list** option in the list settings. This makes the normal list email address(es) work from outside your network as well as internally. Note that if the incoming mail arrives via a POP3 mail collector, then VPOP3 uses the **Accepted Domains** setting for the collector, instead of the **Local Domains** setting, when calculating the default email addresses for the list. This option is not available for *Group* lists.
- You can create one or more [Mappings](#) for the list. This will make the list be available using the **Mapping** email address(es) to both internal and external users (as determined by the rules for the **Mapping**). This option *can* be used to make Groups publicly accessible.

5.2.2 List Types

Distribution Lists

A Distribution List is a simple list containing zero or more email addresses (local or remote).

Mailing Lists

A Mailing List has a lot more features than a distribution list. For instance, a mailing list supports user subscription and removal from the list, modifying message headers to support discussion lists, banning people from lists, and so on.

Another advantage of Mailing Lists over Distribution Lists is that VPOP3 expands Mailing Lists in the background while it expands Distribution Lists immediately. This means that if you send a message to a Distribution List with a large number of local users, it may take a while for VPOP3 to respond to your email client, but sending to an equivalent Mailing List will have an almost instantaneous response.

Forwardings

Forwardings are not really 'lists', because they can only contain a single email address, but they are managed here because they are, essentially, just a special case of a Distribution List, but with only a single member.

ODBC Mailing Lists

ODBC Mailing Lists are only available in VPOP3 Enterprise.

An ODBC Mailing List is a list where all the members are retrieved from an external ODBC database. VPOP3 cannot manage the list members - that has to be done outside of VPOP3 - but the other features of Mailing Lists are supported.

Groups

A Group is a separate type of list which can be used for administrative purposes. For instance, you can set that all members of a particular group cannot send outgoing messages. You can also send emails to all of a group's members, as with a distribution list, but this will only work internally.

Some permissions (eg with calendar sharing in VPOP3 Enterprise) can use a group as the 'target' of the permission - for instance, you could set it so that all members of the 'sales' group have permission to read someone's calendar.

Each user can only be in at most one group, and this is set in the user's settings, rather than in the group settings.

5.2.3 Administering Lists

To administer Lists click on the Lists button at the top of the administrator pages. You can add or remove lists by clicking on the New and Delete buttons at the top of the list of Lists.

To edit a particular list, you can double-click on the list name in the list of Lists. Each type of list has different settings you can manage

- [Distribution Lists](#)
- [Mailing Lists](#)

- [Forwardings](#)
- [ODBC Mailing Lists](#) (External DB Mailing List)
- [Groups](#)

5.2.3.1 Distribution Lists

A Distribution List is a simple list, so there are not many options for this type of list. If you require more options, or more functionality, then consider using a [Mailing List](#) instead. A Mailing List can do all that a Distribution List can do, and more.

For details on the setting tabs, see the sections below:

- [General tab](#)
- [Members tab](#)

To create a Distribution List, go to [Lists](#) on the tool bar and press the **New** button.

Add List Wizard (Page 1)

This Wizard takes you through the simple process of creating a new List in VPOP3.

Please enter the **Name** for the List you are creating. This name is usually the part of the list's email address before the @ symbol. The name must not conflict with another list or user's name.

List Name :

List Comment :

Select the type of list to create:

Distribution List 

Forwarding 

Mailing List 

Enter the list name in the **List Name** box. This is usually the part of the email address before the @ symbol that you will use to send a message to the list members.

Select **Distribution List** as the list type to create. Press **Next**.

Add List Wizard (Page 2 of 2)

When adding a distribution list the only settings needed are whether the list can be accessed by email downloaded from a remote POP3 server, and the list of members.

Allow Internet access to list (Allow incoming mail to be sent to the list)

List Members

Put one email address per line in the box below - blank lines are ignored

fred@example.net

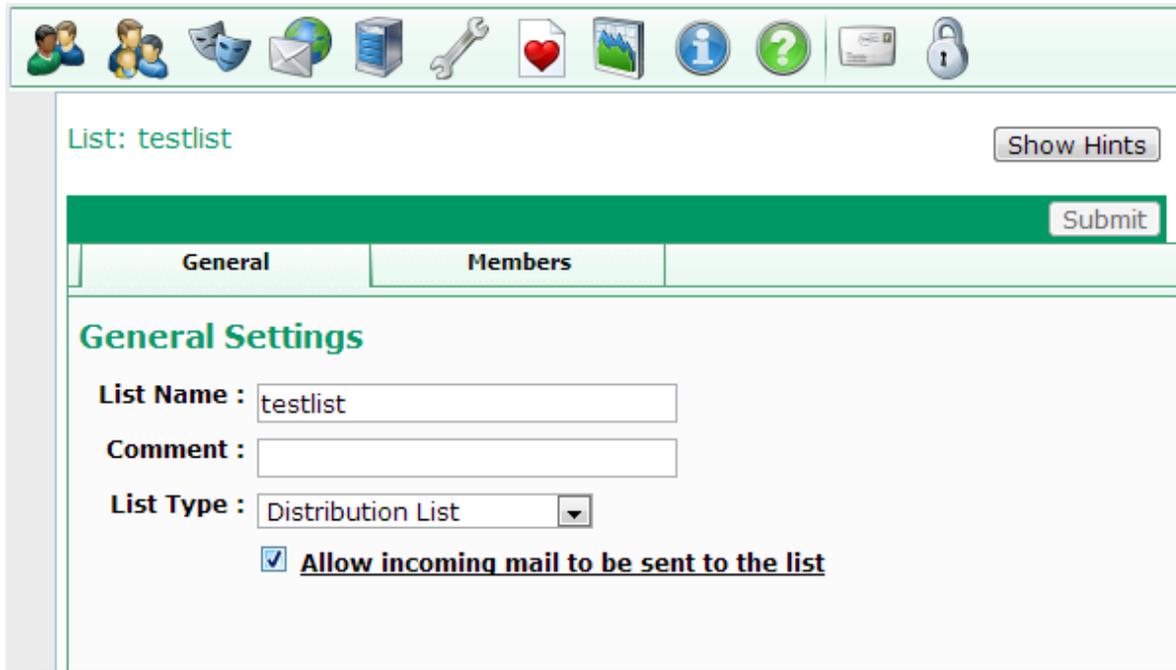
Check the **Allow Internet access to list** box if you want to allow external users to send messages to the list, or leave it cleared if you only want internal VPOP3 users to be able to send to the list.

In the **List Members** box enter the email addresses of the initial members. Press **Finish**.

All the list settings can be changed after creation.

5.2.3.1.1 General

This is the [Distribution List](#) → General Tab



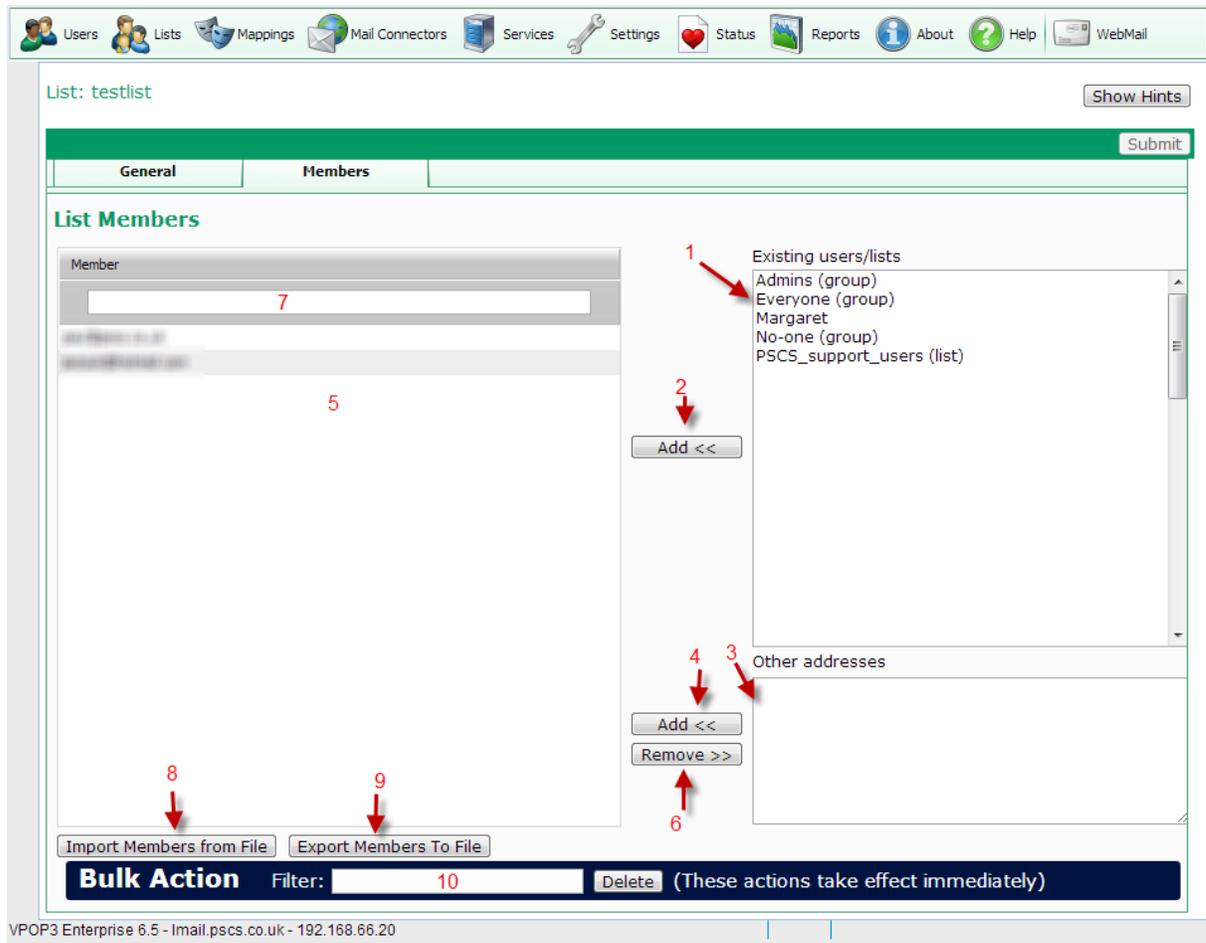
The screenshot shows the 'General' tab of a Distribution List configuration page. At the top, there is a navigation bar with icons for users, mail, server, tools, heart, landscape, info, help, mail, and lock. Below this, the page title is 'List: testlist' with a 'Show Hints' button. A green bar contains a 'Submit' button. Below the bar are two tabs: 'General' (selected) and 'Members'. The 'General Settings' section includes:

- List Name :** testlist
- Comment :** (empty text box)
- List Type :** Distribution List (dropdown menu)
- Allow incoming mail to be sent to the list**

- **List Name** - this is the name of the list. This also defines the [default email address](#) of the list. The list will be called <List Name>@<your domain(s)>
- **Comment** - this is an optional comment for the list. This is only for your use, so can be whatever you want it to be
- **List Type** - as this is a distribution list, it will be set to Distribution List. If you want to change the type of list, you can choose the new type here, and press the Submit button.
- **Allow incoming mail to be sent to the list** - if this option is checked, then external senders can send messages to the list, which will then be distributed to all the list members. If this option is not checked, then only local senders can send messages to the list; messages from external senders will be treated as if the list's email address is not recognised

5.2.3.1.2 Members

This is the [Distribution List](#) → Members Tab



The Distribution list **Members** tab lets you define which email addresses are in the list. Whenever a message is sent to the list, it is BCCd to all the list members.

You can add local users or other lists by selecting them from the list at the top-right of the page (1) and pressing the **Add** button (2)

You can add external email addresses by typing them in the box at the bottom-right of the page (3) and press the **Add** button (4). You can add multiple email addresses at once by typing multiple lines - one email address per line

You can remove email addresses (local or external) from the list by selecting them in the list members box (5) and pressing the **Remove** button (6).

All the above actions only take effect when you press the **Submit** button.

The box (7) lets you filter the members in the list, helping you to find entries if the list of members is large. This uses a simple case-insensitive substring search.

The **Import Members from File** option (8) lets you import the member list from a plain text file (one email address per line). You can choose to merge the imported list with the current members, or replace the current members with the imported list.

The **Export Members to File** button (9) lets you download a list of members as a plain text file (one email address per line).

The **Bulk Action** section lets you delete list members using [wildcards](#) or [regular expressions](#). In the search box (10) you can enter an expression using * and ? wildcards directly, or enter a regular expression surrounded by '/' characters (e.g. /@baddomain\.com/i) This action takes effect immediately. The search & delete actions are performed on the server, so will only apply to members which are already stored on the server, and will delete members from the list stored on the server. When you press the **Delete** button, you will be told how many list members will be deleted by the action and given chance to confirm or reject the action at that point.

5.2.3.2 Mailing Lists

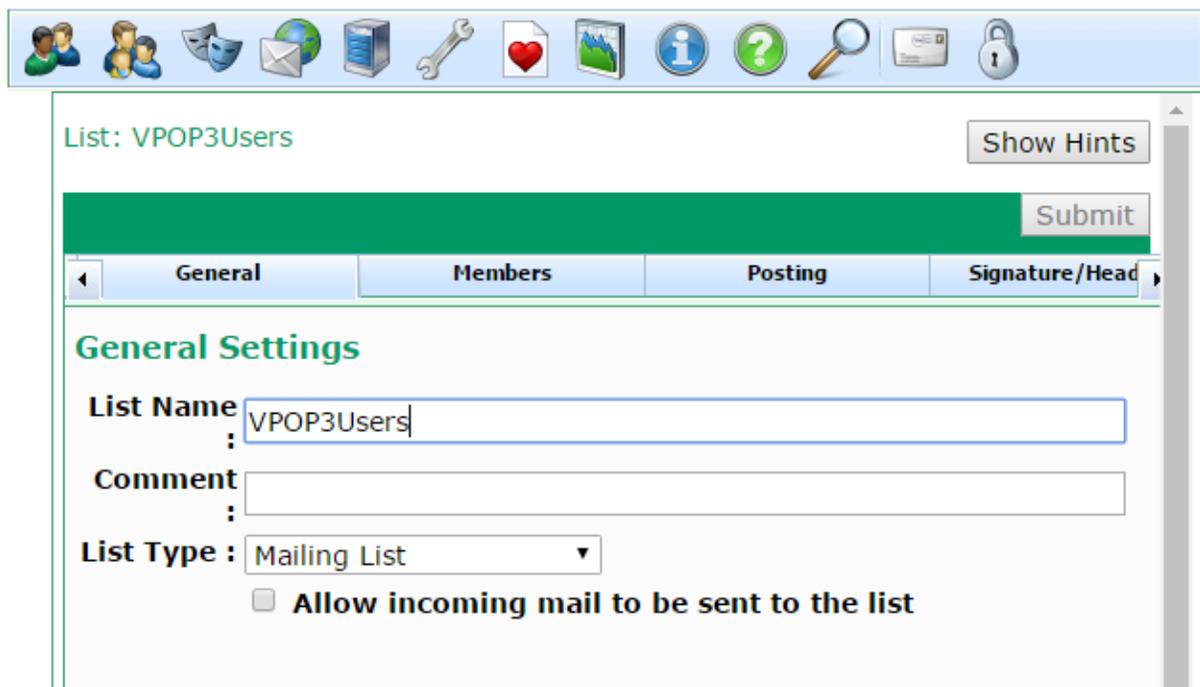
A Mailing List is a flexible list object with many options available. It can be used in place of more basic lists, such as [Distribution Lists](#) if you need extra functionality. Common uses are announcement lists, discussion lists as well as general distribution lists with more features.

For details on the setting tabs, see the sections below:

- [General tab](#)
- [Members tab](#)
- [Posting tab](#)
- [Signature/Header tab](#)
- [Subscriptions tab](#)
- [Other tab](#)

5.2.3.2.1 General

This is the Lists → [Mailing List](#) → General Tab



The screenshot shows the 'General Settings' tab for a mailing list named 'VPOP3Users'. The interface includes a toolbar with various icons (users, mail, server, tools, heart, landscape, info, help, search, mail, lock) and a 'Show Hints' button. Below the toolbar is a green bar with a 'Submit' button. The 'General Settings' section contains the following fields:

- List Name:** VPOP3Users
- Comment:** (empty text box)
- List Type:** Mailing List (dropdown menu)
- Allow incoming mail to be sent to the list**

- **List Name** - this is the name of the list. This also defines the [default email address](#) of the list. The list will be called <List Name>@<your domain(s)>
- **Comment** - this is an optional comment for the list. This is only for your use, so can be whatever you want it to be
- **List Type** - as this is a mailing list, it will be set to Mailing List. If you want to change the type of list, you can choose the new type here, and press the Submit button.
- **Allow incoming mail to be sent to the list** - if this option is checked, then external senders can send messages to the list, which will then be distributed to all the list members. If this option is not checked, then only local senders can send messages to the list; messages from external senders will be treated as if the list's email address is not recognised

5.2.3.2.2 Members

This is the Lists → [Mailing List](#) → Members Tab

The Mailing list **Members** tab lets you define which email addresses are in the list. Whenever a message is sent to the list, it is sent to all the list members (using BCC unless '[Slow Message Posting](#)' is enabled)

You can add local users or other lists by selecting them from the list at the top-right of the page (1) and pressing the **Add** button (2)

You can add external email addresses by typing them in the box at the bottom-right of the page (3) and press the **Add** button (4). You can add multiple email addresses at once by typing multiple lines - one email address per line

You can remove email addresses (local or external) from the list by selecting them in the list members box (5) and pressing the **Remove** button (6).

All the above actions only take effect when you press the **Submit** button.

The box (7) lets you filter the members in the list, helping you to find entries if the list of members is large. This uses a simple case-insensitive substring search.

The **Import Members from File** option (8) lets you import the member list from a plain text file (one email address per line). You can choose to merge the imported list with the current members, or replace the current members with the imported list.

The **Export Members to File** button (9) lets you download a list of members as a plain text file (one email address per line).

The **Bulk Action** section lets you delete list members using [wildcards](#) or [regular expressions](#). In the search box (10) you can enter an expression using * and ? wildcards directly, or enter a regular expression surrounded by '/' characters (e.g. /@baddomain\.com/i) This action takes effect immediately. The search & delete actions are performed on the server, so will only apply to members which are already stored on the server, and will delete members from the list stored on the server. When you press the **Delete** button, you will be told how many list members will be deleted by the action and given chance to confirm or reject the action at that point.

5.2.3.2.3 Signature/Headers

This is the Lists → [Mailing List](#) → Signature/Headers Tab

This tab lets you configure a message signature and header modifiers for mailing list messages sent to list members.

The **List Signature** is text which is added to the bottom of messages sent to the list members. This is plain text only (no HTML) and could contain information such as how to unsubscribe from the list, or list rules, etc.

Message Header Modifiers indicate modifications which VPOP3 will make to the message header of messages sent to the list members.

The default modifiers are a sensible starting point. You can change the header modifiers to change how replies to list messages are handled, and to remove things like receipt requests or add mailing list header fields.

If this is blank, then no header modifications are made. This means that the list members will receive the same headers that the originator sent (with some control & status headers added by VPOP3 and other mail servers). This may be what you wish, but often it isn't. For instance, replies will go back to the original sender, not to the list, and if the original sender asked for read receipts, then they will receive a receipt from every list member, which may be a lot of receipts.

So, you can tell VPOP3 to change the headers - for instance:

- *Reply-to:mylist@example.com* indicates that replies should go back to the 'mylist@example.com' rather than the original sender.
- *Return-Receipt-To:* indicates that VPOP3 should remove any 'Return-Receipt-To' headers to help prevent read receipts being generated.
- *Precedence: bulk* should tell automatic responses not to fire, so that all list members aren't bombarded with out-of-office replies from list members.

etc

If you are configuring a subscription mailing list of some sort, for instance, for discussions, it can be worth adding the standard list header fields, such as List-Unsubscribe and List-Help. See [RFC 2369](#) for details of these header fields, for instance, a header:

```
List-Unsubscribe: <mailto:listserver@example.com?subject=unsubscribe+mylist>
```

can be used to tell the receiving mail software how to generate an email to unsubscribe from the list.

Header modifiers are defined as *Header-Field ":" Header-Data*

If you want VPOP3 to remove a header field, just specify it as *Header-Field ":"* without any data

Common email header fields are documented in [RFC 2076](#).

5.2.3.2.4 Subscriptions

This is the Lists → [Mailing List](#) → Subscriptions Tab

The screenshot shows the VPOP3 web interface for configuring a mailing list. The top navigation bar includes icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, and Search. The main content area is titled 'List: AllUsers' and has a 'Show Hints' button. Below this is a 'Submit' button and a tabbed interface with tabs for General, Members, Posting, Signature/Headers, Subscriptions (selected), and Other. The Subscriptions tab contains the following settings:

- Allow people to subscribe to the list themselves
- Inform the list moderator(s) of any new subscriptions or unsubscriptions
- Inform the list moderator(s) of any unsubscriptions
- Verify list subscriptions by sending an email to the new subscriber asking them for confirmation
- This list is *confidential* (it will not appear in any list directory)
- Use a custom welcome message
- Send welcome message when moderator adds list member

Below the checkboxes are three text input fields:

- ListServer for this list :** *
- Custom Welcome Message :** To remove yourself from this list, send a message to ListServer@pscs.co.uk containing the single line unsubscribe AllUsers
- Custom Unsubscribe Message :** Use a custom unsubscribe message
Unsubscription from "AllUsers" succeeded

At the bottom of the interface, the status bar shows: VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 | Idle | In: 39757 | Out: 0

The Mailing list **Subscriptions** tab lets you configure how VPOP3 allows and handles list subscription and unsubscription requests.

The **Allow people to subscribe to the list themselves** option allows people to email listserver@<your domain> with a message containing 'subscribe <listname>' in the message subject or content to add themselves to the list membership. If this is not checked, then only a VPOP3 administrator or list moderator can add members.

The **Inform the list moderators of any new subscriptions or unsubscriptions** option tells VPOP3 to send a message to the list moderator(s) (defined on the [Other](#) tab) when someone subscribes to or unsubscribes from the list.

The **Inform the list moderators of any unsubscriptions** option tells VPOP3 to send a message to the list moderator(s) (defined on the [Other](#) tab) when someone unsubscribes from the list.

The **Verify list subscriptions** option sends an email to someone who subscribes to the list, asking them to confirm that they wish to join the list. This is recommended nowadays to prevent people being added to lists without their knowledge.

The **This list is confidential** option means that the results of the Listserver Lists command will not include this list.

The **Use a custom welcome message** option means that VPOP3 will send the contents of the **Custom Welcome Message** box to a new subscriber to the list, instead of a basic built-in message.

The **Send a welcome message when moderator adds list member** option means that VPOP3 will send the welcome message when a moderator adds a member, as well as when the member subscribes themselves. If this is not checked, the a welcome message is only sent when someone subscribes themselves.

The **ListServer for this list** option is only available in [VPOP3 Enterprise](#). This indicates which Listserver manages this mailing list. For instance, if your VPOP3 handles multiple domains, you may want different list servers for the different domains. "*" means the generic Listserver@<local domain> address is used, otherwise enter the email address of the list server you wish to create or use.

The **Custom Welcome Message** box lets you create a custom message which is sent to new list subscribers.

The **Use a custom unsubscribe message** option means that VPOP3 will send the contents of the **Custom Unsubscribe Message** box to someone who unsubscribes from the list, instead of a basic built-in message.

The **Custom Unsubscribe Message** box lets you create a custom message which is sent to people who unsubscribe from the list.

5.2.3.2.5 Other

This is the [Mailing List](#) → Other Tab

The screenshot shows the 'Other' tab of the 'resellers_onstop' mailing list settings. The interface includes a 'Show Hints' button and a 'Submit' button. The 'Other' tab is selected, showing various configuration options:

- Allow Remote Administration (by email)
- Allow list members to request a list of members from the ListServer
- Slow Message Posting (individual messages to each recipient, rather than one message BCC'd to them all)
- List Moderator: support
- Return Address: resellers_onstop_owner@psecs.co.uk (this is where bounce messages are sent)
- Spam Threshold: -1 (if this is '-1' then no spam filtering will occur for this list)
- Spam Redirection: (email address(es) where detected spam for this list will be sent)
- List Digests**
A list digest is a second mailing list which has messages automatically sent to it periodically containing all the messages sent to the main list.
- This list is a digest of: <None>
- Archive messages to this list (needed if this is to have a digest)
- Generate digest messages every: 1 days
- Keep archive messages for: 1 days

The **Allow Remote Administration** option lets list moderators send email messages to the **ListServer** to manage the list - for instance, to add or remove list members. See the **Remote Administration** topic for details.

The **Allow list members to request a list of members from the ListServer** option allows list members to send a **Users <listname>** command to the **ListServer** to see a list of members on the list. Usually this will be turned off, but in small, closed, lists it may be useful.

The **Slow Message Posting** option will make VPOP3 send messages to list members individually rather than as a single message which is BCCd to all list members. This has the advantage that each message has the recipient listed in the **To** header field, but it has the disadvantage that it takes longer to process the messages, and VPOP3 will have to send out the same message many times, so on a slow Internet connection this may take a while.

The **List Moderator** indicates a user or distribution list which is the 'moderator' for the list. The moderator may have extra powers over the list, for instance, only the moderator may be allowed to post to the list, or moderators may have to approve messages to the list or moderators may be able to add/remove people from the list. If you select a single user as the moderator, then that user is the moderator. If you select a distribution list, then every member of that list is a moderator.

The **Return Address** is the location where bounce messages will be sent in response to failed outgoing mailing list messages.

The **Spam Threshold** indicates whether spam filtering will take place for this list, and, if so, the spam score threshold at which messages will be treated as spam. -1 indicates no spam filtering, 100 is the spam threshold for normal spam filtering.

The **Spam Redirection** option indicates where detected spam for this list will be sent (if the Spam Threshold is not -1) because only users have spam quarantines in VPOP3 - lists do not have quarantine. If this option is blank then spam to the list is just discarded, otherwise it is sent to the specified email address(es), and if they are VPOP3 users, it will probably be quarantined for those users.

List Digests

A List Digest can be useful for discussion mailing lists. A list digest will group up messages over a certain period and send them as one message. So, you may have a daily digest for a discussion mailing list which will mean that, each day, a single message will be sent to subscribers of the digest list containing all the messages that were sent on the previous day.

If you select a list in the **This list is a digest of ...** option, then VPOP3 will create a digest of the *selected list's* messages and distribute it to members of *this list*. So, you are configure a mailing list called 'mylist_digest' and you select **This list is a digest of: mylist**, then VPOP3 will create a message containing all the messages sent to the 'mylist' list and send that message to members of the 'mylist_digest' list. Multiple lists can be digests of a single list - for instance, you may want to have a daily and a weekly digest of a list.

The **Archive messages to this list** option tells VPOP3 to keep messages distributed by this list for future reference. This is needed if you are going to create digest lists based on this list. So, in the above example, this option would need to be enabled for the 'mylist' list.

The **Generate digest messages every X days** option tells VPOP3 how often to create the digest messages

The **Keep archive messages for X days** option tells VPOP3 how long to keep the archived messages for this list. This must be at least as long as the longest '**Generate digest messages every...**' option for any lists which are digest lists of this list. So, in the example above, if the **mylist_digest** list has **Generate digest messages every 7 days** selected, then the **Keep archive messages for X days** option for the **mylist** list must be set to at least 7 days.

5.2.3.3 Forwardings

A 'Forwarding' is a special case of a [Distribution List](#) which just has a single member.

If you create a Forwarding called "joe" with a Forwarding Address of "bob@example.com", then any messages sent to the address joe@<local domain> will be forwarded on to bob@example.com.

You can also forward messages using the [Routing tab](#) in a user's settings, but that way uses a user licence, whereas using a Forwarding doesn't.

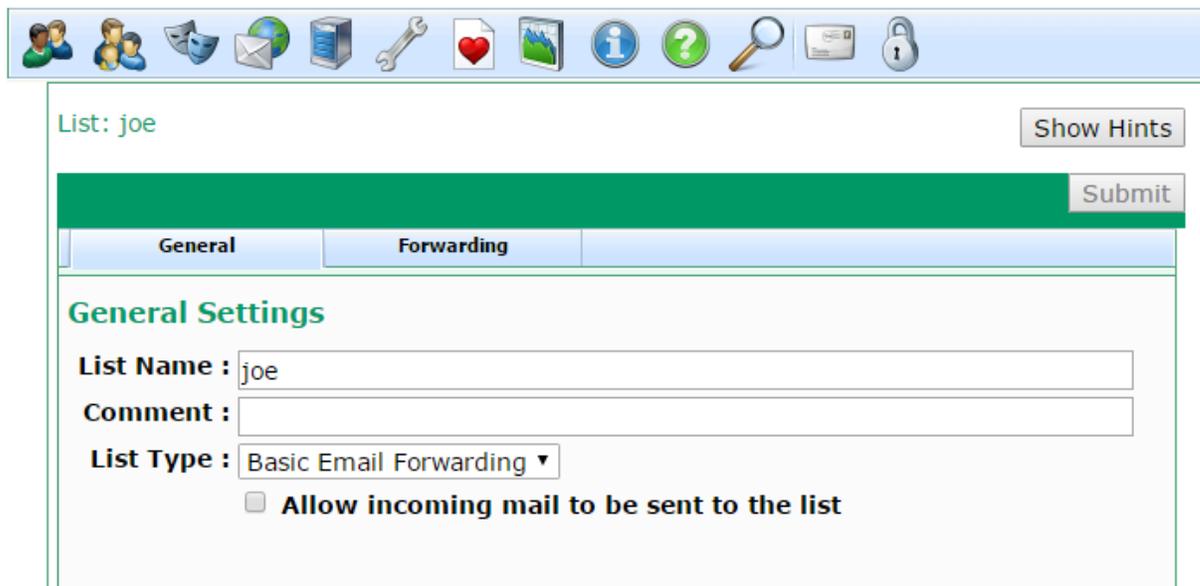
For details on the setting tabs, see the sections below:

➤ [General tab](#)

➤ [Forwarding tab](#)

5.2.3.3.1 General

This is the Lists → [Forwarding](#) → General Tab



List: joe Show Hints

Submit

General **Forwarding**

General Settings

List Name : joe

Comment :

List Type : Basic Email Forwarding ▾

Allow incoming mail to be sent to the list

- **List Name** - this is the name of the Forwarding list. This also defines the [default email address](#) of the list. The list will be called <List Name>@<your domain(s)>
- **Comment** - this is an optional comment for the list. This is only for your use, so can be whatever you want it to be
- **List Type** - as this is a forwarding, it will be set to Forwarding. If you want to change the type of list, you can choose the new type here, and press the Submit button.
- **Allow incoming mail to be sent to the list** - if this option is checked, then external senders can send messages to the list, which will then be distributed to the Forwarding Address. If this option is not checked, then only local senders can send messages to the list; messages from external senders will be treated as if the list's email address is not recognised

5.2.3.3.2 Forwarding

This is the Lists → [Forwarding](#) → Forwarding Tab

The screenshot shows the configuration page for a list named "joe". At the top, there is a navigation bar with various icons. Below it, the list name "List: joe" is displayed next to a "Show Hints" button. A green banner indicates "Changes have been made - press: Submit". The "Forwarding" tab is selected, showing the "Forwarding Address" field with the value "bob@example.com".

The Forwarding **Forwarding** tab lets you define the email address which messages to this Forwarding list will be distributed to. You can only specify a single email address here. If you wish to use more, then change the list type to a [Distribution List](#). (In VPOP3, a Forwarding is just a special case of a Distribution List where there is just one list member).

The **Forwarding Address** is the email address where messages to this List will be forwarded to. It can be a local or remote email address.

5.2.3.4 ODBC Mailing Lists

An ODBC Mailing List is very similar to a normal [Mailing List](#), except that the members list is held in, and retrieved from, an external database (using an ODBC connector), not the VPOP3 database. For instance, you may already have a database with a list of your customers, so using this mechanism means that you can create a mailing list which obtains your customer list dynamically from this external database.

However, this also means that you cannot manage the members list from the VPOP3 settings, and people cannot subscribe to or unsubscribe from the list via VPOP3.

You can configure the ODBC link by using the **Configure ODBC** link on the **Members** tab.

VPOP3 obtains the members list from the external database as needed, so the external database must be always available.

For details on the setting tabs, see the sections below:

- [General tab](#)
- [Members tab](#)
- **Posting** tab
- [Signature/Header tab](#)

➤ [Other tab](#)

5.2.3.4.1 General

This is the Lists → [Mailing List](#) → General Tab

The screenshot shows the 'General Settings' tab for a mailing list named 'VPOP3Users'. The interface includes a toolbar with various icons (users, mail, server, tools, heart, landscape, info, help, search, mail, lock) and a 'Show Hints' button. Below the toolbar is a green bar with a 'Submit' button. A tabbed interface shows 'General', 'Members', 'Posting', and 'Signature/Head' tabs. The 'General Settings' section contains the following fields:

- List Name:** A text input field containing 'VPOP3Users'.
- Comment:** An empty text input field.
- List Type:** A dropdown menu set to 'Mailing List'.
- Allow incoming mail to be sent to the list**

- **List Name** - this is the name of the list. This also defines the [default email address](#) of the list. The list will be called <List Name>@<your domain(s)>
- **Comment** - this is an optional comment for the list. This is only for your use, so can be whatever you want it to be
- **List Type** - as this is a mailing list, it will be set to Mailing List. If you want to change the type of list, you can choose the new type here, and press the Submit button.
- **Allow incoming mail to be sent to the list** - if this option is checked, then external senders can send messages to the list, which will then be distributed to all the list members. If this option is not checked, then only local senders can send messages to the list; messages from external senders will be treated as if the list's email address is not recognised

5.2.3.4.2 Signature/Headers

This is the Lists → [Mailing List](#) → Signature/Headers Tab

This tab lets you configure a message signature and header modifiers for mailing list messages sent to list members.

The **List Signature** is text which is added to the bottom of messages sent to the list members. This is plain text only (no HTML) and could contain information such as how to unsubscribe from the list, or list rules, etc.

Message Header Modifiers indicate modifications which VPOP3 will make to the message header of messages sent to the list members.

The default modifiers are a sensible starting point. You can change the header modifiers to change how replies to list messages are handled, and to remove things like receipt requests or add mailing list header fields.

If this is blank, then no header modifications are made. This means that the list members will receive the same headers that the originator sent (with some control & status headers added by VPOP3 and other mail servers). This may be what you wish, but often it isn't. For instance, replies will go back to the original sender, not to the list, and if the original sender asked for read receipts, then they will receive a receipt from every list member, which may be a lot of receipts.

So, you can tell VPOP3 to change the headers - for instance:

- *Reply-to:mylist@example.com* indicates that replies should go back to the 'mylist@example.com' rather than the original sender.
- *Return-Receipt-To:* indicates that VPOP3 should remove any 'Return-Receipt-To' headers to help prevent read receipts being generated.
- *Precedence: bulk* should tell automatic responses not to fire, so that all list members aren't bombarded with out-of-office replies from list members.

etc

If you are configuring a subscription mailing list of some sort, for instance, for discussions, it can be worth adding the standard list header fields, such as List-Unsubscribe and List-Help. See [RFC 2369](#) for details of these header fields, for instance, a header:

```
List-Unsubscribe: <mailto:listserver@example.com?subject=unsubscribe+mylist>
```

can be used to tell the receiving mail software how to generate an email to unsubscribe from the list.

Header modifiers are defined as *Header-Field ":" Header-Data*

If you want VPOP3 to remove a header field, just specify it as *Header-Field ":"* without any data

Common email header fields are documented in [RFC 2076](#).

5.2.3.4.3 Other

This is the [Mailing List](#) → Other Tab

List: resellers_onstop Show Hints

Submit

General	Members	Posting	Signature/Headers	Subscriptions	Other
---------	---------	---------	-------------------	---------------	-------

Allow Remote Administration (by email)
 Allow list members to request a list of members from the ListServer
 Slow Message Posting (individual messages to each recipient, rather than one message BCC'd to them all)

List Moderator: support ▼
Return Address: resellers_onstop_owner@pscs.co.uk (this is where bounce messages are sent)
Spam Threshold: -1 (if this is '-1' then no spam filtering will occur for this list)
Spam Redirection:
 (email address(es) where detected spam for this list will be sent)

List Digests
 A list digest is a second mailing list which has messages automatically sent to it periodically containing all the messages sent to the main list.

This list is a digest of: <None> ▼
 Archive messages to this list (needed if this is to have a digest)

Generate digest messages every: 1 ▼ days
Keep archive messages for: 1 ▼ days

The **Allow Remote Administration** option lets list moderators send email messages to the **ListServer** to manage the list - for instance, to add or remove list members. See the **Remote Administration** topic for details.

The **Allow list members to request a list of members from the ListServer** option allows list members to send a *Users <listname>* command to the **ListServer** to see a list of members on the list. Usually this will be turned off, but in small, closed, lists it may be useful.

The **Slow Message Posting** option will make VPOP3 send messages to list members individually rather than as a single message which is BCCd to all list members. This has the advantage that each message has the recipient listed in the **To** header field, but it has the disadvantage that it takes longer to process the messages, and VPOP3 will have to send out the same message many times, so on a slow Internet connection this may take a while.

The **List Moderator** indicates a user or distribution list which is the 'moderator' for the list. The moderator may have extra powers over the list, for instance, only the moderator may be allowed to post to the list, or moderators may have to approve messages to the list or moderators may be able to add/remove people from the list. If you select a single user as the moderator, then that user is the moderator. If you select a distribution list, then every member of that list is a moderator.

The **Return Address** is the location where bounce messages will be sent in response to failed outgoing mailing list messages.

The **Spam Threshold** indicates whether spam filtering will take place for this list, and, if so, the spam score threshold at which messages will be treated as spam. -1 indicates no spam filtering, 100 is the spam threshold for normal spam filtering.

The **Spam Redirection** option indicates where detected spam for this list will be sent (if the Spam Threshold is not -1) because only users have spam quarantines in VPOP3 - lists do not have quarantine. If this option is blank then spam to the list is just discarded, otherwise it is sent to the specified email address(es), and if they are VPOP3 users, it will probably be quarantined for those users.

List Digests

A List Digest can be useful for discussion mailing lists. A list digest will group up messages over a certain period and send them as one message. So, you may have a daily digest for a discussion mailing list which will mean that, each day, a single message will be sent to subscribers of the digest list containing all the messages that were sent on the previous day.

If you select a list in the **This list is a digest of ...** option, then VPOP3 will create a digest of the *selected list's* messages and distribute it to members of *this list*. So, you are configure a mailing list called 'mylist_digest' and you select **This list is a digest of: mylist**, then VPOP3 will create a message containing all the messages sent to the 'mylist' list and send that message to members of the 'mylist_digest' list. Multiple lists can be digests of a single list - for instance, you may want to have a daily and a weekly digest of a list.

The **Archive messages to this list** option tells VPOP3 to keep messages distributed by this list for future reference. This is needed if you are going to create digest lists based on this list. So, in the above example, this option would need to be enabled for the 'mylist' list.

The **Generate digest messages every X days** option tells VPOP3 how often to create the digest messages

The **Keep archive messages for X days** option tells VPOP3 how long to keep the archived messages for this list. This must be at least as long as the longest '**Generate digest messages every...**' option for any lists which are digest lists of this list. So, in the example above, if the **mylist_digest** list has **Generate digest messages every 7 days** selected, then the **Keep archive messages for X days** option for the **mylist** list must be set to at least 7 days.

5.2.3.5 Groups

In the **Lists** area of the VPOP3 administration, you cannot administer groups at all. This is because a group is not really a list, but many people think of them as lists, so they are included in the **Lists** area for convenience.

All you can see in the **Lists** section is the list of [users](#) in the group. Groups can only contain local users. There are two types of groups: built-in groups, and custom groups.

Built-in groups

There are three built-in groups in all installations of VPOP3:

- **Everyone** - this usually contains all users, but you can remove a user from the Everyone list by editing the user, and going to the [Permissions tab](#), then unchecking the **Put user in Everyone list** option
- **Admins** - this contains all users who are administrators. You cannot remove or add users from this group except by altering their Administrator status (by editing the user, and going to the [General tab](#), and setting the **Administrator** option).
- **No-one** - this contains no-one. You cannot add users to this group. This group can be useful if you want to have some messages simply disappear. For instance, you could create a [Mapping](#) of a certain email address to No-one, to have messages addressed to that email address simply vanish.

Custom groups

Administrators can create custom groups on the [Settings » Groups](#) page. Groups define certain behaviour for a group of users. Each user can only be in one custom group at once (but they can be in as many Lists as you want)

To add or remove a user from a group, edit the user, and choose the group from the **Group** drop-down list on the [General](#) tab. You can remove a user from all groups, by selecting the **<None>** entry from the list.

5.3 Mappings

The **Mappings** tab in the VPOP3 settings lets you specifically associate email addresses with users.

Email Address	Target	Type	Collector	Comments
sales	Albert	Always	All Mail Collectors	

VPOP3 Enterprise 6.20 - pscs2.co.uk - FD00:F0F2:498F:5FF2:2480:EC9C:A597:6EAD

(Also see the [Mappings Definition](#) topic)

If you don't do anything else, then VPOP3 automatically associates <username>@<domain> with the user 'username'. The <domain> part depends on the situation - for internal or incoming SMTP mail, the <domain> is the [Local Domains](#) setting, for incoming POP3 mail the <domain> is the [Accepted Domains](#) setting. So, if the **Local Domains** is set to *example.com*, then a local message to *fred@example.com* will be routed to the user called 'fred'.



Tip

If you want to disable these default associations, then you can turn them off in the [Local Mail](#) settings or the Mail Collector [Routing Options](#) as appropriate.

Mappings let you change this default association of email addresses -> users. So, you can add or override email address -> user associations.

A Mapping of **sales** -> **albert** will mean that mail to **sales@<domain>** will be delivered to the VPOP3 User **albert**. You do not need a VPOP3 User called 'sales' for this to work.

If you *do* have a VPOP3 User called 'sales', then this Mapping will stop mail addressed to **sales@<domain>** being delivered to that User, the mail will **ONLY** go to the User **albert**. If you want the mail to go to both users, then you will need to create a second Mapping of **sales** -> **sales** as well. (Or use a [Distribution List](#)).

Wildcard Mappings

[Wildcards](#) (* and ?) can be used in Mappings, but note that, because Mappings take precedence, you have to take care. For instance, if your Local Domain is *example.com*, then a Mapping of ***@example.com** -> **bob** will mean that the User **bob** will receive all messages, even if they are addressed to other users. In this case VPOP3 will *not* deliver the message to the original recipient and also copy it to **bob** - it will *only* send the message to **bob**. You could create explicit Mappings for your other users to send messages for those addresses to those users as well as copying the messages to **bob**.

Unrecognised Address Mappings

There is a special 'wildcard' which can be used in Mappings - the tilde (~). If this is placed as the only thing before the @ symbol in the Mapping, then VPOP3 interprets it as "unrecognised addresses @", so if you have two users **kate** and **joe**, and a single Mapping of **~@example.com** -> **joe**, then messages to **kate@example.com** will be delivered to **kate**, and messages to any other **address@example.com** will be delivered to **joe** because of the tilde Mapping.



Tip

The **How VPOP3 determines message recipients** topic contains more detailed information on how VPOP3 calculates the recipients of a message.

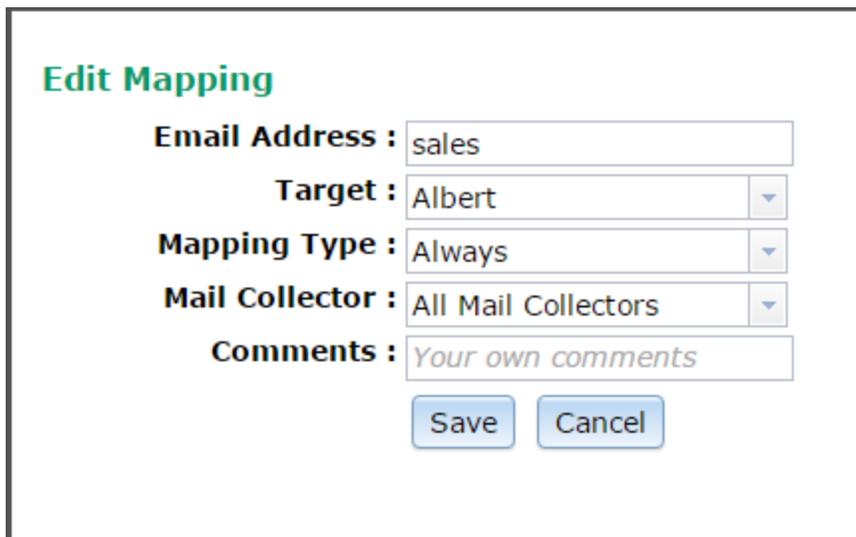
*REMOTE Mappings

Another special type of Mapping is a Mapping to the special ***REMOTE** value, for instance **Mark -> *REMOTE**. This type of Mapping tells VPOP3 that the address **Mark** exists, but is not in this VPOP3 installation. That means that if a local user sends a message to **Mark@localdomain**, then VPOP3 won't reject it as for an unrecognised recipient, instead VPOP3 will put the message into the Outqueue to be sent to the Internet. Also, if a VPOP3 [Mail Collector](#) downloads a message for **Mark@domain** from a remote POP3 mailbox, then VPOP3 will just ignore that recipient rather than treating it as an unrecognised recipient.

This can be useful if you have more than one mail server handling mail for your domain. You can use *REMOTE mappings in VPOP3 for the email addresses handled by the other mail server.

Adding/Editing Mappings

To add a Mapping, press the **New** button, and to edit a Mapping double-click on it.



Edit Mapping

Email Address : sales

Target : Albert

Mapping Type : Always

Mail Collector : All Mail Collectors

Comments : *Your own comments*

Save Cancel

In the **Email Address** box put the email address for the Mapping. You can use the full email address, wildcards or ~ as described above, or just the name part of a local email address.

In the **Target** box choose who you want to receive messages for the specified email address, or you can select *REMOTE if appropriate (see above).

The **Mapping Type** option lets you choose when the Mapping will apply:

- **Always** - the Mapping will always apply
- **POP3** - the Mapping will apply to messages downloaded using a POP3 [Mail Collector](#).
- **SMTP** - the Mapping will apply to messages received using SMTP.
- **FROM** - the Mapping will apply to messages downloaded using a POP3 Mail Collector, but VPOP3 will check the *sender's* email address rather than the recipient's email address.

If the Mapping Type is **POP3**, then you can specify which **Mail Collector** the Mapping applies to (or **All Mail Collectors**).

The **Comments** box lets you enter comments for your own reference.

Import / Export Mappings

At the bottom of the Mappings page are two buttons to Export the Mappings to a CSV file or Import Mappings from a CSV file.

The CSV file has five columns:

1. Email Address
2. Target mailbox/list
3. Comment
4. Type (Normal, POP3, SMTP or FROM)
5. Mail Collector ID (or 'ALL')

When importing a file, only the first 2 columns are required. If the others are omitted, then these settings are assumed: blank comment, 'Normal' type and 'ALL' collectors

5.4 Mail Connectors

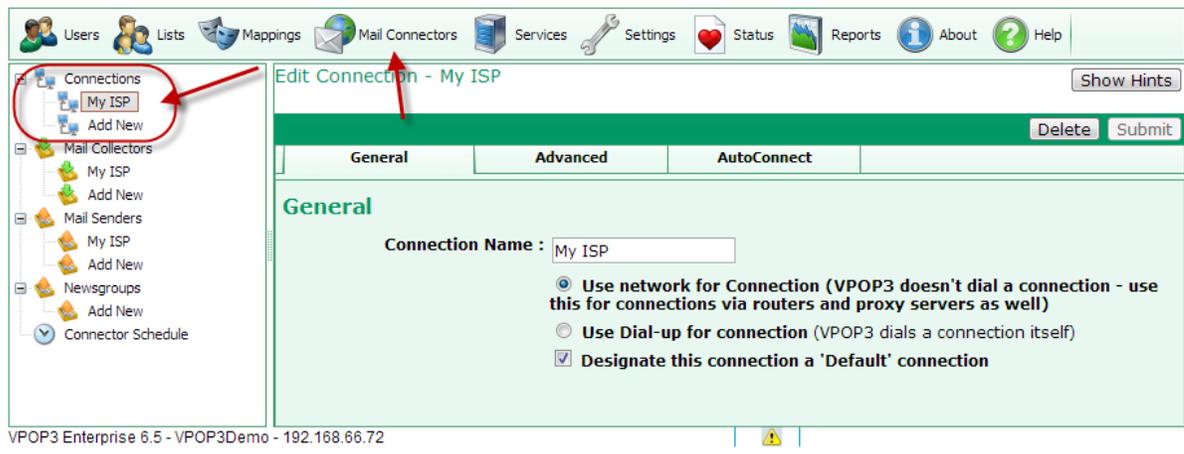
Mail Connectors tell VPOP3 how to connect to the Internet, how to send & retrieve email, and how often to connect.

See the [Mail Connectors](#) topic in the General Concepts section for an overview of the different types of objects here, and the following topics for details of the VPOP3 settings pages related to Mail Connectors.

5.4.1 Connections

In VPOP3 a [Connection](#) tells VPOP3 how to connect to the Internet.

Nowadays, this will usually just be set to "connect via a router", which is the normal choice for connections over cable, xDSL, leased lines, satellite, Wifi, etc. In most cases, you will just have a single **Connection**, which is usually created by the [Setup Wizard](#)



To access the **Connection** settings, click on the **Mail Connectors** button on the top of the VPOP3 settings screen, then see the **Connections** section of the tree on the left of the screen.

To [add a new Connection](#), click on the **Add New** option under the **Connections** section.

To [edit or view a Connection](#), select the relevant **Connection**, then look at the settings in the right-hand side of the screen.

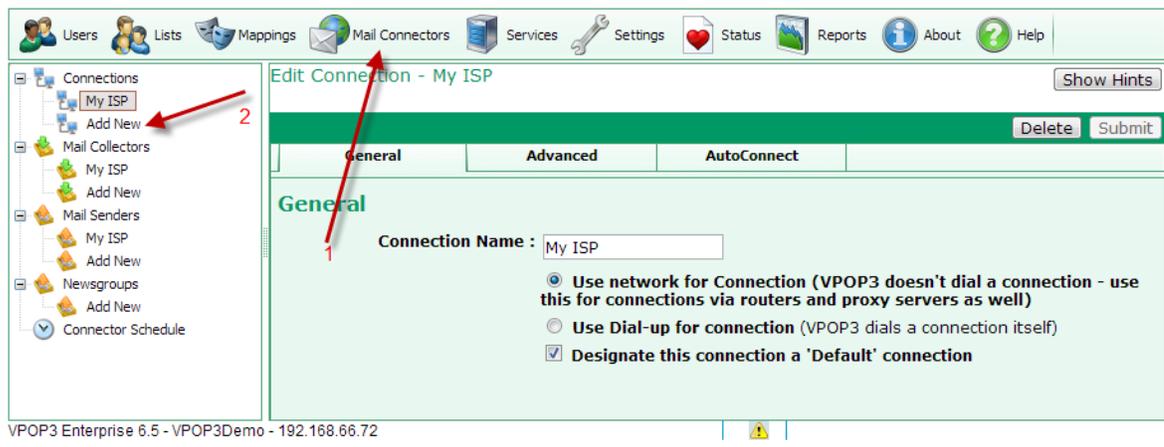
To delete a **Connection**, select the relevant **Connection**, then click on the **Delete** button at the top-right of the **Connection** settings.

Advanced uses of Connections

In some cases you may want to have multiple **Connections**, even if you only have one way of physically connecting to the Internet. Some examples are:

- If you have to be able to send different mail out using different **Mail Senders**. Because each **Mail Sender** is associated with a different **Connection**, you need to create multiple **Connections** to do this.
- If you want to have a more complex **Schedule**, where different **Mail Collectors** or **Mail Senders** are used at different intervals, you can create multiple **Connections**, and associate them with different **Collectors**. The **Schedule** tells VPOP3 when to trigger each **Connection**.

5.4.1.1 Add a Connection



To add a **Connection**, click on the **Mail Connectors** button on the top of the VPOP3 settings screen, then press **Add New** in the **Connections** section at the left of the screen.

This will bring up a Wizard which will take you through the configuration of a new **Connection** and associated **Mail Sender**.

All the settings made by the Wizard can be altered later by [editing the Connection](#).

Add Connection

This Wizard takes you through the simple process of adding a new Connection method to your VPOP3 settings. Connection methods tell VPOP3 how to connect to the Internet (or a remote private network). Each Connection method optionally has an associated Out Mail method which you can also configure using this Wizard. It does not tell VPOP3 how to collect mail - that is set in the Mail Collector configurations

Please enter the **name** for the Connection method you are creating. This name is used when displaying the settings to you and when reporting any error messages or status information. The name can be anything you want, but it is best to make it meaningful - for instance the name of your Internet provider, or remote network etc.

Connector Name :

To use this Connection method, should VPOP3 use a LAN connection (for instance, through a router, proxy server or firewall) or should it initiate its own dial-up connection using a modem or ISDN terminal adapter?

LAN Connection
 Dial-up Connection (RAS)

Should this Connection method use the main schedule? If you choose not, then this Connection method will either have to be controlled using a separate schedule, or controlled manually.

Use with Main Schedule

In **Connector Name**, type the name you want to use for this **Connection**. The actual value does not matter, but it will be used by VPOP3 in status & error messages, so it is best to make it something meaningful - such as the name of your Internet provider

In the next section, choose whether this **Connection** will be a **LAN connection** (e.g. via a router) or a **dial-up connection** (e.g. via a modem). Most connections will be LAN connections nowadays.

Check the **Use with Main Schedule** box if this is a **Connection** which you want to use your normal connection schedule. This option can be altered later by changing the **Designate this connection a 'Default' connection** option [in the Connection's settings](#).

Press **Next >>** to go to the next page

➤ Next page for **LAN Connection**

➤ Next page for **Dial-up Connection**

5.4.1.2 Edit a Connection

To edit a [Connection](#), go to the VPOP3 settings, click on **Mail Connectors** at the top of the page, then select the appropriate **Connection** from the [Connections](#) section at the left of the page.

You will see 3 or 4 tabs depending on the type of **Connection** you are viewing.

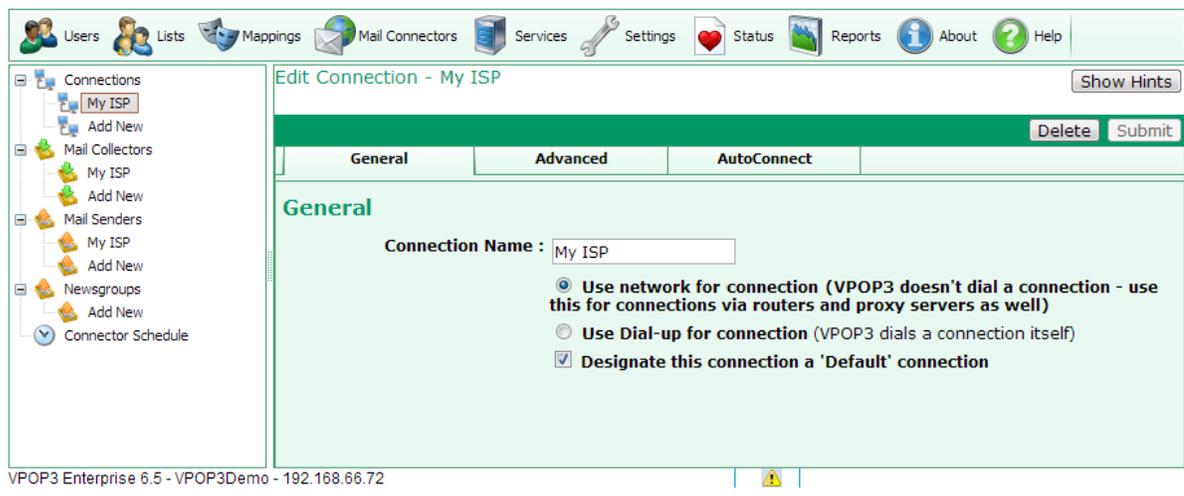
LAN Connection

- [General](#)
- [Advanced](#)
- AutoConnect

Dial-up Connection

- [General](#)
- Dial-up
- [Advanced](#)
- AutoConnect

5.4.1.2.1 General



The **Connection » General** tab lets you set the basic options for a [Connection](#) method. For most people, this is the only tab you will need to access.

The **Connection Name** is the name which you have given the **Connection** method. The actual value of the name does not matter, but it is used in logging and status messages, so it is useful to use a meaningful name, such as the name of your Internet provider.

Choose the **Use network for connection** option if your VPOP3 will be connecting to the Internet via a router (the usual case). VPOP3 will not control the connection in any way, and will assume that the connection is always available. Note that you do not need to tell VPOP3 anything else about your Internet connection, such as router details or subnet masks. This is all handled by the Windows network settings.

Choose the **Use Dial-up for connection** option if you want VPOP3 to control a modem to connect and disconnect from the Internet as required. This option is rarely used nowadays, but is still available in case it is necessary.

Check the **Designate this connection a 'Default' connection** box if you want this **Connection** to be triggered using your normal [Connector Schedule](#). Note that this is only a convenience feature - in **Schedule** items you can tell VPOP3 to connect to specific **Connections** or to connect to **Default Connections**. By using the **Default Connection** feature, you can change which **Connections** are used by editing the Connection itself, rather than by editing the schedule. Both methods are equivalent, but some people find one way more convenient than the other.

Dial-up connection notes

The modem must be connected to the VPOP3 computer. If the modem is installed on a separate PC, then use the **Use network for connection** option in VPOP3, and install proxy server software or routing software (e.g. the Internet Connection Service) on that other PC, The details of this are outside the scope of this documentation.

Because VPOP3 generally runs as a service, which is in a different user account from the currently logged in user, any dial-up connections must have been created as usable by any user on the PC, otherwise they will not be visible to VPOP3. How to do this depends on which version of Windows you are using.

In Windows 7:

1. Go to **Control Panel**
2. Choose **Network and Sharing Center**
3. Choose **Set up a new connection or network**
4. Choose **Set up a dial-up connection**, press **Next**
5. Set up the settings as normal, but make sure that the **Allow other people to use this connection** box is checked. (Note that we don't know any way to set an existing connection to be usable by other people, so it appears that you can only do this when creating the dial-up connection)

5.4.1.2.2 Advanced

To get to this page, to Mail Connectors → (choose Mail Connection) → Advanced.

Edit Connection - My Sender Show Hints

Delete Submit

General Advanced AutoConnect

Advanced Settings

Dial-up connections which can also be used for this connection method if already established :

VPN Connection
VPN Connection 2

Connect through SOCKS Proxy Server

If this connection fails totally, try another Connection : <None>

Note that VPOP3 detects a failed connection as one where no outgoing TCP/IP connections have succeeded, so it will think that an 'incoming SMTP' mail account with no outgoing mail to send has failed, because no outgoing connections have been tried and succeeded

s.co.uk - 192.168.66.23 | Idle | In: 40743 | Out: 0

This page lets you set advanced settings for a connection method. The settings on this page are not normally needed.

The **Dial-up connections which can also be used for this connection method if already established** option lets you tell VPOP3 that if it detects a dial-up connection is in use when VPOP3 wants to use the current connection method, then VPOP3 can just use the detected dial-up connection instead of trying to make a new dial-up connection. This option is only needed if VPOP3 is using a dial-up connection to connect to the Internet and the computer has several dial-up connections configured which can be used for sending/collecting mail.

The **Connect through SOCKS proxy server** option tells VPOP3 that when this Connection method is used, VPOP3 should make connections through the SOCKS proxy server defined in the [Misc Settings](#) rather than connecting directly to the remote servers.

The **If this connection fails totally, try another Connection** option tells VPOP3 that if *all* the Mail Senders and Mail Collectors associated with this Connection method fail, then VPOP3 should connect again, immediately using a different Connection method.

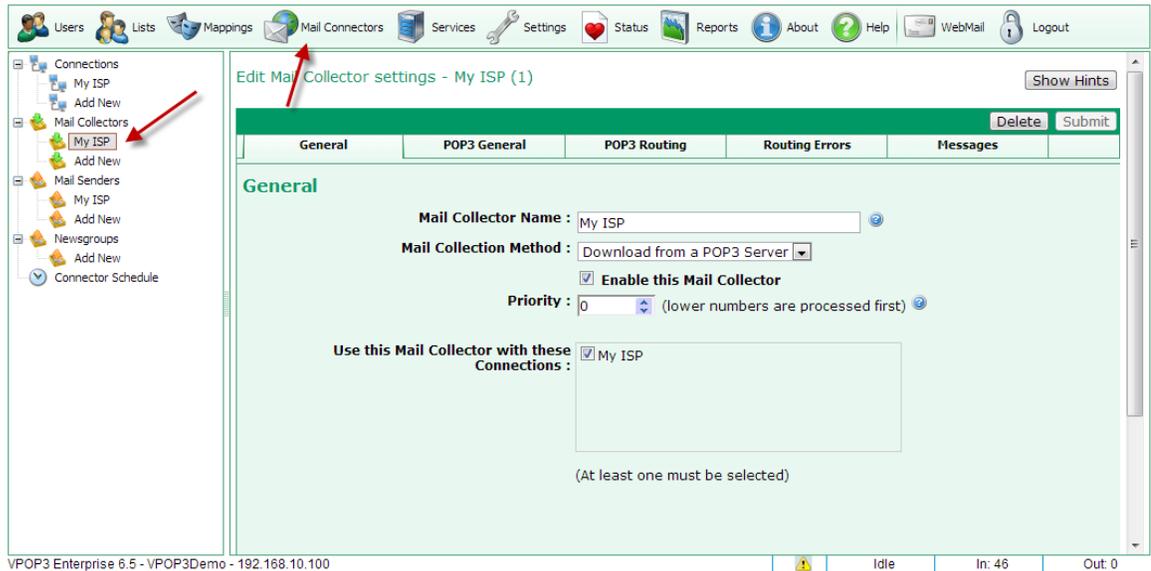
One example of where this may be useful is if you normally have VPOP3 connecting through a router, but you also have a 3G dongle in the VPOP3 computer. You could have two Connections defined in VPOP3 - one using the router ('LAN') and the other controlling the 3G dongle using dial-up networking. The normal [Connection Schedule](#) in VPOP3 would use the LAN connection, but you could use this option to have VPOP3 connect using the 3G dongle if the LAN connection fails totally.

Note that this option is normally *not* useful to detect which of two router connections is in use, because VPOP3 has no way of knowing what the router is doing. For instance, if the router has the 3G dongle in

it, and the router has fallen back to using 3G instead of xDSL, then VPOP3 has no way of knowing this, so it will still use the LAN connection.

5.4.2 Mail Collectors

In VPOP3 a [Mail Collector](#) tells VPOP3 how to retrieve messages from the Internet.



Screenshot

To access the **Mail Collector** settings, click on the **Mail Connectors** button on the top of the VPOP3 settings screen, then see the **Mail Collectors** section of the tree on the left of the screen.

To [add a new Mail Collector](#), click on the **Add New** option under the **Mail Collectors** section.

To [edit or view a Mail Collector](#), select the relevant **Mail Collector**, then look at the settings in the right-hand side of the screen.

To delete a **Mail Collector**, select the relevant **Mail Collector**, then click on the **Delete** button at the top-right of the **Mail Collector** settings.

Tip

Note that for a direct incoming SMTP feed, you usually do not need to create a Collector. VPOP3 is always listening for incoming SMTP connections, so an incoming SMTP mail feed should 'just work' if you have your router configured correctly.

5.4.2.1 Add a Mail Collector

The screenshot displays the VPOP3 Admin Settings interface. The top navigation bar includes icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, WebMail, and Logout. The left sidebar shows a tree view with 'Mail Collectors' selected, and a red arrow points to the 'Add New' button under 'My ISP'. The main content area is titled 'Edit Mail Collector settings - My ISP (1)' and features a 'Show Hints' button. Below the title are 'Delete' and 'Submit' buttons. The 'General' tab is selected, showing the following configuration:

- Mail Collector Name:** My ISP
- Mail Collection Method:** Download from a POP3 Server
- Enable this Mail Collector**
- Priority:** 0 (lower numbers are processed first)
- Use this Mail Collector with these Connections:** My ISP

(At least one must be selected)

VPOP3 Enterprise 6.5 - VPOP3Demo - 192.168.10.100

To add a **Mail Collector**, click on the **Mail Connectors** button on the top of the VPOP3 settings screen, then press **Add New** in the **Mail Collectors** section at the left of the screen.

This will bring up a Wizard which will take you through the configuration of a new **Mail Collector**.

All the settings made by the Wizard can be altered later by [editing the Mail Collector](#).

Add Mail Collector (Page 1 of 4)

This Wizard takes you through the simple process of adding a new Mail Collector to your VPOP3 settings. Mail Collectors tell VPOP3 how to collect email messages from the Internet (or another private mail server). They do not tell VPOP3 how to connect to the Internet or send mail - those settings are defined in the Connection and Mail Sender configurations.

Please enter the **name** for the Mail Collector you are creating. This name is used when displaying the settings to you and when reporting any error messages or status information. The name can be anything you want, but it is best to make it meaningful - for instance the name of your Internet provider, or account name etc.

Mail Collector Name :

To retrieve mail should VPOP3 download mail from a POP3 mailbox, accept incoming SMTP mail or collect from an ODMR (ATRN) server?

- POP3 Download**
 Incoming SMTP
 ODMR Collection

<< Back

Next >>

Cancel

In **Mail Collector Name**, type the name you want to use for this **Mail Collector**. The actual value does not matter, but it will be used by VPOP3 in status & error messages, so it is best to make it something meaningful - such as the name of your Internet provider or email account.

In the next section, choose whether this **Mail Collector** will collect mail from an external **POP3 mailbox**, or with a polled **SMTP** connection, or using **ODMR** (also known as ATRN).

Press **Next >>** to go to the next page

- Next page for **POP3 Download**
- Next page for **Incoming SMTP**
- Next page for **ODMR Collection**

5.4.2.2 Edit a Mail Collector

If you click on a Mail Collector in the Mail Connectors tree, you can edit how VPOP3 collects incoming mail.

There are different options depending on the type of Mail Collector you have, and the settings for that Collector. The type of Collector is set on the **General** tab

Download from a POP3 Server

- [General Tab](#)
- [POP3 General Tab](#)
- [POP3 Routing Tab](#)
- [Routing Errors Tab](#) (optional)
- [Messages Tab](#)

Incoming SMTP Mail Feed

- [General Tab](#)
- [SMTP Options Tab](#)

ODMR (ATRN) Mail Collection

- [General Tab](#)
- [ODMR Options Tab](#)

5.4.2.2.1 General

To get to this page, to Mail Connectors → (choose Mail Collector) → General.

This page sets the basic settings for a Mail Collector.

The screenshot displays the 'Edit Mail Collector settings - MyISP (1)' page in the VPOP3 Enterprise 6.20 Admin Settings. The interface includes a top navigation bar with icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. A left-hand navigation tree shows the hierarchy: Connections (My Connection2, test2, Add New Connection), Mail Collectors (DRSmith, SMTP In, MyISP, Add New Collector, Import Collectors), Mail Senders (My Connection2, test2, Add New Sender), Newsgroups (Bob, Add New News Collector), and Connector Schedule. The main content area has tabs for General, POP3 General, POP3 Routing, Routing Errors, and Messages. The 'General' tab is selected, showing the following settings:

- Mail Collector Name:** MyISP
- Mail Collection Method:** Download from a POP3 Server
- Enable this Mail Collector**
- Priority:** 20 (lower numbers are processed first)
- Use this Mail Collector with these Connections:** My Connection2, test2

At the bottom, a red error message states: "Last connection result: Error from remote server on "PASS *****" -> -ERR authorization failed". The status bar at the bottom shows "VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23" and "Idle | In: 46204 | Out: 1".

A Mail Collector tells VPOP3 how to collect incoming mail.

The **General** tab sets some basic settings. The other tabs for this Collector will depend on what settings are chosen here.

The **Mail Collector Name** is a name you have given this Collector. It doesn't mean anything to VPOP3, but is simply used in the settings and any error messages to help you find which Collector it is talking about.

The **Mail Collection Method** tells VPOP3 how this Collector collects mail. There are three options:

- **Download from a POP3 Server**
- **Incoming SMTP Mail Feed**
- **ODMR (ATRN) Mail Collection**

Your ISP will have told you which option to choose. In most cases it will be **Download from a POP3 Server**. **ODMR (ATRN)** is quite rare; even though it is technologically superior to POP3, it is designed for collection by email servers such as VPOP3 rather than directly by email clients, so most ISPs do not support it.

The **Incoming SMTP Mail Feed** option is only needed if VPOP3 has to "do something" for the SMTP Mail Feed to work - eg send an ETRN command or trigger a dial-up connection. Most [incoming SMTP mail feeds](#) just happen automatically. In that case, you do not need to create a Mail Collector in VPOP3, it will just work.

The **Enable this Mail Collector** option will stop this Mail Collector working if it is turned off. (Note that this will NOT stop an incoming SMTP mail feed if it doesn't need VPOP3 to do anything, it will just stop VPOP3 performing its actions to trigger the incoming messages).

The **Priority** option lets you re-order the Mail Collectors, so that some will come before others. VPOP3 will process the lower number priorities first. Note that generally this is not needed. If you have VPOP3 collecting [every 10 minutes](#), then it doesn't matter whether a particular Collector is processed first or last, it will still be processed approximately every 10 minutes.

The **Use this Mail Collector with these Connections** tells VPOP3 which [Connections](#) this Collector should be used with. This can be useful if you need to have different Collectors act with different frequencies. See the [Connection Scheduling section](#) for more information.

The **Last connection result** section shows the result of the last time this Collector tried to work.

5.4.2.2.2 POP3 General

To get to this page, to to Mail Connectors → (choose Mail Collector) → POP3 Routing. This tab is only available if the **Mail Collection Method** on the [General tab](#) is set to **Download from a POP3 Server**.

This page tells VPOP3 how to retrieve messages from your email service provider.

Edit Mail Collector settings - (1) Show Hints

Changes have been made - press: Delete Submit

General POP3 General POP3 Routing Routing Errors Message

POP3 General Settings

If you do not know the settings below, you should contact your ISP or email hosting provider for the details.

POP3 Server Address : Port: (Default is 110)

POP3 Account Username :

POP3 Account Password :

Session Encryption :

POP3 Authentication Method : (make sure the POP3 server supports the selected method)

Maximum Message Size To Download : kB (set to 0 for no limit)

Leave Messages on Server : days (set to 0 to delete immediately)

Use Download Rules to filter downloaded messages

Attempt to remove duplicate messages (within a single session of this Mail Collector)
If you want VPOP3 to check for duplicates across multiple sessions, or multiple mail collectors, see Global Duplicate Detection on Settings -> Misc

The **POP3 server address**, **POP3 Account Username**, and **POP3 Account Password** will all be supplied by your Internet provider, and could be anything they say they should be. We often get asked "is the account name my email address" - the answer is: "possibly". Some Internet providers will use your email address, some will use the part of your email address before the @ symbol, and some will use a totally unrelated name. There is no way for us to help with this - contact your ISP.

The **Port** number is usually 110 if your Internet provider uses standard POP3. A few ISPs use a deprecated, non-standard, 'POP3S' system which is on port 995. If your Internet provider does this, then set the **Port** to 995, and in the **Session Encryption** box, choose **SSL**.

The **Session Encryption** method says how the session/connection between VPOP3 and your ISP should be encrypted:

- **None** means that the connection is not encrypted. Your messages (and possibly login details) are sent in plain text.
- **SSL** means that the connection is encrypted as soon as it connects. This method usually uses an alternate port (995) and is non-standard and deprecated.
- **STLS** means that the connection starts off unencrypted, and then VPOP3 sends the **STLS** command to the remote server to switch to encrypted mode as soon as it connects. This is the standard way of supporting session encryption, and uses the normal port 110. If the remote server doesn't support the **STLS** command, then VPOP3 will refuse to connect.
- **STLS if available** means that the connection starts off unencrypted. VPOP3 checks to see if the remote server supports the **STLS** command. If it does, VPOP3 will send that command to switch to encrypted mode. If the remote server does not support **STLS**, then VPOP3 will continue without encrypting the session.

The **POP3 Authentication Method** option tells VPOP3 how to log onto the remote server:

- *Plain Text* means that VPOP3 sends the login details using plain text. (If the session is encrypted, then the plain text will be contained in the encrypted session, so will be encrypted).
- *APOP* uses a simple challenge-response one way hash algorithm to make it harder to see the password if an unencrypted session is spied upon.
- *CRAM-MD5* is an alternative challenge-response algorithm which also makes it harder to spy on the password.
- *MSN (SPA)* is a proprietary Microsoft authentication method which has been used for some Microsoft mail services. As far as we know, this is no longer required.
- *Compuserve (RPA)* is a proprietary Compuserve authentication method. This requires RPA software from Compuserve to work. As far as we know, this is no longer required.

When choosing an authentication method, make sure that your Internet provider supports the chosen method. Contact your Internet provider for help if you are uncertain.

The **Maximum message size to download** option tells VPOP3 what the maximum message size to download is. This is set in kB (1kB = 1024 bytes). Set this value to 0 for no limit. If VPOP3 detects a message larger than the specified size, it will leave the message on the Internet provider. If **Use Download Rules** is checked, then VPOP3 will send a message to the original recipients telling them of the large message. The message contains instructions about how the user can reply to the message to download the message at the next connection. If **Use Download Rules** is not checked, then VPOP3 will send a message to the **pop3downloadtoobig** message target (set in Settings → [Admin Settings](#) → [Message Targets](#)), this message will tell that user about the big message, but there is no option to download the message in this case.

The **Leave Messages on Server** option tells VPOP3 to leave messages on the Internet provider's mail server for the specified number of days (specify "0" for VPOP3 to download the messages immediately). Note that some Internet providers have a mailbox size limit, so leaving messages there too long may mean you reach that limit and do not receive new messages. Also, leaving messages on your Internet provider too long will slow down message collection; in POP3 there is no 'new message' concept, so VPOP3 cannot simply request new messages when it connects, it has to download a list of all the messages which are on your Internet provider, and work out which ones it has seen before. This requires a POP3 feature called *UIDL* - most Internet providers nowadays support this feature, but if your Internet provider doesn't, you should disable this option by setting it to "0".

The **Use Download Rules** option tells VPOP3 to use the defined **Download Rules** to provide preliminary filtering of messages in the Internet provider's mailbox. **Download Rules** allow you to ignore messages, delete them from the Internet provider immediately, redirect them, ask if they should be downloaded, etc. These actions can only be chosen based on the message *headers*, not based on message content (including attachments) because they are processed before the message is downloaded into VPOP3. Use the [spam/content filter scripting](#) if you need to filter messages based on message content.

Press the **Edit Download Rules** button to [edit the Download Rules](#).

The **Attempt to remove duplicate messages** option tells VPOP3 to check for apparent duplicated messages within this particular session to the Internet provider. This is most useful if you have a catch-all POP3 account, and your Internet provider (or the sender) puts a copy of a message into the mailbox for each recipient if a message is CC'd to several people at your company. Note that VPOP3 will play safe here, so if your Internet provider (or the sender) changes the message slightly for each copy, VPOP3 may not be able to detect that they are duplicates. We worked on the principle that it is better to get duplicates than to miss messages totally.

5.4.2.2.2.1 Download Rules

To get to this page, go to Mail Connectors → (choose Mail Collector) → POP3 Routing → Edit Download Rules

This page lets you configure rules for how VPOP3 processes messages it downloads from a remote POP3 server.

Name	Action	Collector	Conditions	Buttons
(No name)	Redirect	All	2 condition(s)	Edit Delete
(No name)	Redirect	All	3 condition(s)	Edit Delete
(No name)	Redirect	All	1 condition(s)	Edit Delete
Download	Download	All	2 condition(s)	Edit Delete
Download	Download	All	2 condition(s)	Edit Delete
Ignore de	Ignore	All	2 condition(s)	Edit Delete
Ignore de	Ignore	All	2 condition(s)	Edit Delete
Ignore de	Ignore	All	2 condition(s)	Edit Delete
Ignore de	Ignore	All	2 condition(s)	Edit Delete
Ignore de	Ignore	All	2 condition(s)	Edit Delete
Ignore de	Ignore	All	2 condition(s)	Edit Delete
Junk from	Ignore	All	1 condition(s)	Edit Delete
	Redirect	All	2 condition(s)	Edit Delete
Redirect j	Redirect	All	2 condition(s)	Edit Delete
Delete rul	Delete and Warn	All	4 condition(s)	Edit Delete
(No name)	Redirect	All	1 condition(s)	Edit Delete
(No name)	Redirect	Any	2 condition(s)	Edit Delete
ask about	Query	All	1 condition(s)	Edit Delete
Redirect &	Redirect, Download and Del	All	1 condition(s)	Edit Delete
Ignore Di	Ignore	Any	27 condition(s)	Edit Delete
(No name)	Redirect	All	1 condition(s)	Edit Delete

VPOP3 processes download rules in order from top to bottom. When it finds a rule whose conditions match the incoming message, it will process the rule, and then stop processing any further messages (except where stated otherwise below in the **Action** descriptions). You can re-order the rules by clicking the up/down arrows to the left of the rule names.

Note that the same Download Rules apply to all POP3 Mail Collectors. Use the **Collector** rule condition if you just want a particular rule to apply to a particular collector. For incoming SMTP use [SMTP Rules](#) instead.

You can add a new rule by pressing the **Add Rule** button at the top of the page, delete a rule by pressing the **Delete** button to the right of the rule name, or edit the rule by pressing the **Edit** button to the right of the rule name. Changes to rules take effect immediately, so there is no **Submit** button; just press the **Close** button to close the editor.

When you add or edit a rule, the rule editor will be displayed as below

Download Rule x

Name:

Action:

Redirect to:

Condition match:

Conditions

<input type="text" value="from"/>	<input type="checkbox"/>	not	<input type="text" value="contains"/>	<input type="text" value="@psecs.co.uk"/>	<input type="button" value="Delete"/>
<input type="text" value="received"/>	<input type="checkbox"/>	not	<input type="text" value="contains"/>	<input type="text" value="from psecs.co.uk by"/>	<input type="button" value="Delete"/>
<input type="text" value="x-authentication-warning"/>	<input type="checkbox"/>	not	<input type="text" value="contains"/>	<input type="text" value="didn't use HELO protocol"/>	<input type="button" value="Delete"/>

The **Name** box contains a name you specify for the rule. The name can be anything, but it is best to make it something meaningful to make the rules easier to maintain and to help when looking in log files.

The **Action** box lets you specify what happens when the rule conditions match. See the Action Descriptions section below for more details.

The **Redirect to** box lets you specify an email address which the message should be redirected to if the rule matches. This box is only present for **Redirect** actions. A similar **Copy to** box is displayed for **Copy** rules. You can specify multiple email addresses by separating them with commas. With VPOP3 Enterprise you can also specify a target folder for local targets by adding a space and the folder name after the username - eg *fred Customers*, *bob* will send it to the "inbox" for the user "bob" and the "Customers" folder for the user "fred".

For **Set Header** actions, there is a **Header Line** box where you can specify the header line to add.

The **Condition match** box lets you specify whether all the conditions must match for the rule to be triggered, or only any one of the conditions must match.

Below this you specify the conditions for the rule. You can specify as many conditions as you want. Press the **Add Condition** button to add a new condition, and delete an existing condition by pressing the relevant **Delete** button. See the Condition Descriptions section below for more details.

Action Descriptions

- **Query** - VPOP3 will send a message to the original recipient(s) of the message showing them the message headers and asking them if they want to download the message. If they reply to the query message, then VPOP3 will download the message during the next POP3 collection. The message on the ISP will be deleted after the [Query Download Delay](#) if the user does not respond to the message.
- **Download** - the message will be downloaded as normal
- **Delete and Warn** - the message will immediately be deleted from the ISP POP3 mailbox and the intended recipient(s) of the message will be told that the message was deleted.
- **Ignore** - the message will not be downloaded from the ISP POP3 mailbox, but it will not be deleted immediately either. It will be deleted when the message ages beyond the [Leave messages on server](#) setting for the Collector.
- **Redirect** - the message will not be delivered to the original recipient(s) but will be redirected to the recipients specified in the Download Rule.
- **Delete Silently** - the message will immediately be deleted from the ISP POP3 mailbox, and no notification about the deletion will be generated.
- **Download and Delete** - the message will be downloaded and delivered as normal, but it will also be immediately deleted from the ISP POP3 mailbox without waiting for the **Leave messages on server** time specified for the Collector.
- **Redirect Query** - VPOP3 will send a message to the recipient(s) specified in the Download Rule showing them the message headers and asking them if they want to download the message. If they reply to the query message, then VPOP3 will download the message during the next POP3 collection. The message on the ISP will be deleted after the [Query Download Delay](#) if the user does not respond to the message.
- **Delete and Warn other user** - the message will immediately be deleted from the ISP POP3 mailbox and the recipient(s) specified in the Download Rule will be told that the message was deleted.
- **Redirect, Download and Delete** - the message will be downloaded and redirected, but it will also be immediately deleted from the ISP POP3 mailbox without waiting for the **Leave messages on server** time specified for the Collector.
- **Copy** - the message will be delivered to the original recipient(s) as well as to the recipients specified in the Download Rule.
- **Copy Query** - VPOP3 will send a message to the original recipient(s) of the message as well as to the recipient(s) specified in the Download Rule showing them the message headers and asking them if they want to download the message. If they reply to the query message, then VPOP3 will download the message during the next POP3 collection. The message on the ISP will be deleted after the [Query Download Delay](#) if the user does not respond to the message.
- **Delete and copy Warning** - the message will immediately be deleted from the ISP POP3 mailbox and the original recipient(s) as well as the recipient(s) specified in the Download Rule will be told that the message was deleted.

- **Copy, Download and Delete** - the message will be downloaded and copied to the specified recipient(s), but it will also be immediately deleted from the ISP POP3 mailbox without waiting for the **Leave messages on server** time specified for the Collector.
- **Headers only** - VPOP3 will download only the message headers (not the message body) and deliver them to the original recipient(s).
- **Redirect Headers only** - VPOP3 will download only the message headers (not the message body) and deliver them to the recipient(s) specified in the Download Rule.
- **Copy Headers only** - VPOP3 will download only the message headers (not the message body) and deliver them to the original recipient(s) as well as to the recipient(s) specified in the Download Rule.
- **Reject** - VPOP3 will send a delivery failure notification to the sender of the message and the message will not be downloaded.
- **Set Header and Continue** - VPOP3 will add a message header to the incoming message. VPOP3 will then continue to process further Download Rules. (Note that the header is modified AFTER the download rules have run, so you cannot check for the changed header in later download rules).
- **Set Header and Stop** - VPOP3 will add a message header to the incoming message. VPOP3 will then not process further Download Rules.
- **If** - if this rule does not match, VPOP3 will not process any more rules until it encounters an **Else** or **EndIf** rule.
- **Else** - this type of rule cannot have any Conditions. It must be used after an **If** rule.
- **EndIf** - this type of rule cannot have any Conditions. It must be used after an **If** or **Else** rule.
- **Stop** - VPOP3 will stop processing any further rules, and the default action will take effect (usually **Download**).

Condition Descriptions

Conditions have 4 parts:

1. the type of condition
2. optional **Not** flag. If this is set, then the match operator is inverted (eg if the match operator is 'Contains', then if you check the **Not** box, the match condition becomes 'Does not contain')
3. match operator (eg Contains, Equals etc)
4. data

Condition Types

The condition type can be ANY message header field, as well as some special pseudo-headers.

Common header fields to check are **From**, **To**, **Subject** etc. Note that if VPOP3 is checking a message header field it does not process the header data, but uses the full data from the raw header. This means that if you check for "**From**" "**Equals**" "**bob@company.com**", it is actually unlikely to match messages from bob@company.com. This is because often the From header would actually say **From: Bob Wright <bob@company.com>**, so VPOP3 will be comparing **Bob Wright <bob@company.com>** to just **bob@company.com**, and they are not equal.

You can check multiple headers by separating them with commas - a common example would be **To,Cc** to check both the To and Cc header fields. If either header matches, then the condition matches.

The pseudo-headers supported by VPOP3 are:

- **Always** - if the data is '1' then the condition matches, if the data is '0' then the condition doesn't match. The actual message data is not checked at all.
- **TimeNow** - this checks if the time now is within the range specified by the condition data. You can specify times as hh:mm or just hh and indicate ranges by using the '-' character. Eg '9:00-17:00' will match if the current time is between 9.00 am and 5.00 pm inclusive or 9-17 will match if the current time is between 9.00am and 5.59 pm. If you do not specify a From time, then 0:00 is assumed. If you don't specify a To time, then 23:59 is assumed. VPOP3 uses the local time on the VPOP3 computer for time checks. The match operator is ignored.
- **DayNow** - this checks if the day of week now is specified in the condition data. Sunday is 1, Monday is 2 etc. So, **DayNow - 135** will match if the current day is Sunday, Tuesday or Thursday. The match operator is ignored.
- **Rcpt** - this checks to see if the recipient specified in the condition data is in the calculated recipients for the message (after Mappings etc have been processed). The match operator is ignored.
- **Collector** - this checks to see if the current Mail Collector name or number is the one specified in the condition data. The match operator is ignored.
- **Size** - this checks to see if the message size matches the condition data as indicated by the match operator.
- **ValidRecipients** - this checks to see if the number of valid recipients for the message matches the condition data as indicated by the match operator.
- **InvalidRecipients** - this checks to see if the number of invalid recipients for the message matches the condition data as indicated by the match operator.
- **Any** - this checks all the message headers against the condition data as indicated by the match operator.

Match Operators

All matches apart from regex matches are case insensitive. Numeric data is checked numerically for numeric operators like **greater than** etc. If you check numeric data with **contains**, **begins with**, **regex** etc, then the numeric data is converted to a string a tested as text.

- **equals** - the value matches the condition data exactly.
- **is** - the same as **equals**
- **not equals** - the value does not match the condition data.
- **greater than** - the value is greater than the condition data (text data is compared alphabetically).
- **greater or equal** - the value is greater than or equal to the condition data (text data is compared alphabetically).
- **less than** - the value is less than the condition data (text data is compared alphabetically).
- **less or equal** - the value is less than or equal to the condition data (text data is compared alphabetically).
- **contains** - the value contains the condition data as a substring.
- **wildcard matches** - the value matches the condition data when processed as a wildcard string (* and ? wildcards).
- **begins with** - the value begins with the condition data.

- **ends with** - the value ends with the condition data.
- **regex matches** - the value matches the specified regular expression - specified as `/<regex>/<flags>` - eg `/my cat/i`

Diagnostics

VPOP3 writes a line to message headers of downloaded messages which are affected by Download Rules. This header line begins with **X-VPOP3Rules**.

Also, VPOP3 creates a log file in the [log_path](#) called **DLRULES.LOG**. This log file contains information on all download rules which are triggered.

5.4.2.2.3 POP3 Routing

To get to this page, to to Mail Connectors → (choose Mail Collector) → POP3 Routing. This tab is only available if the **Mail Collection Method** on the [General tab](#) is set to **Download from a POP3 Server**.

This page gives you five options of how VPOP3 will handle the messages it downloads from the POP3 server. Each of these options may have further options as described below.

Route by parsing message headers

POP3 Routing Options

Choose how you want VPOP3 to route incoming messages which it downloads using this Mail Collector. The most common options are "Route according to detected recipient" for catch-all mailboxes, or "Send all messages to a specified user/list" for individual mailboxes.

Route by parsing message headers. This option is usually used where the POP3 mailbox is used for multiple local users (e.g. catch-all mailboxes). The **Accepted Domains** setting tells VPOP3 which email domains or addresses to expect in this POP3 account. Separate multiple entries with ';' (semicolon) characters.

Accepted Domains :

Send all messages to a specified user/list. This option is usually used where the POP3 mailbox is used for a single local user.

When this option is chosen VPOP3 will download a message, then look through the message headers of the downloaded message to try to work out who the message is for, and it will then deliver the message to the relevant local user(s). By default VPOP3 will look in the To, Cc, Received and Apparently-To headers to see who the message is for. It will find all the email addresses listed there, and compare them to the **Accepted Domains** setting configured for this option. You can specify multiple entries in the **Accepted Domains** setting by separating the entries with semicolons.

This option is usually used if your ISP provides you with a *catch-all* mailbox.

Accepted Domains entries can be:

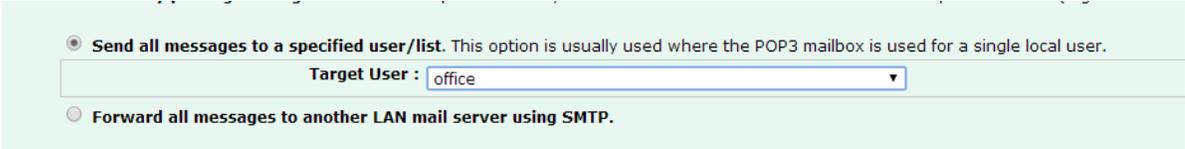
- Domain - just specify your domain name - eg `pscs.co.uk` or `example.org`. You can use wildcards here if you wish, but they are rarely useful.
- Email address - specify the full email address, or use wildcards, eg `fred@example.com` or `joe.*@example.org`

Some people have been tempted to use a wildcard as the domain entry - eg `*` - thinking that they want VPOP3 to process all email domains it sees (maybe they have lots of domains). This is generally not a good idea. It works OK as long as people **ONLY** send messages to your domains, but if a message is sent to you, and CCd to someone at a different company, VPOP3 will try to process the CC email address as well, and will either generate an error message, or deliver the message to someone who shouldn't have received it.

One problem with this type of message routing is that [BCCd messages generally cannot be delivered automatically](#). This is because the BCC recipients are not put into the message header, so VPOP3 cannot see who the message was for. Depending on your ISP, you may be able to customise the message routing options to make this work, but there is no guarantee this will be possible (it relies on your ISP doing non-standard things).

The [Configure Routing Options](#) button lets you configure advanced rules for routing messages. Generally you will not need to use these options, but in a few cases you might.

Send all messages to a specified user/list



Send all messages to a specified user/list. This option is usually used where the POP3 mailbox is used for a single local user.

Target User :

Forward all messages to another LAN mail server using SMTP.

When this option is chosen, VPOP3 will simply route all messages which it downloads using this mail collector to the user or list which you specify.

This option is usually used if your ISP provides you with one mailbox for each of your local users.

All you need to do is choose the appropriate user or list in the **Target User** box

Forward all messages to another LAN mail server using SMTP



Forward all messages to another LAN mail server using SMTP.

Target email address :

Target email server :

(This forwards to a single email address on the other mail server. To forward to different email addresses on the other mail server use the Main LAN forwarding configuration on **Local Mail -> LAN Forwarding**)

Attempt to work with a single email address by detecting text name or comment in address fields if possible (not recommended if it is at all poss

When this option is chosen, VPOP3 will send all messages which it downloads using this mail collector to a specified email address on another mail server on your network.

This option is usually used if your ISP provides you with one mailbox for each of your local users and you want VPOP3 to send the messages to another mail server. If you want the messages to go to another mail server, but your ISP provides you with a catch-all account, then use the **Route by parsing message headers** option and either use [LAN Forwarding](#) or have the mail go to VPOP3 users who then [forward on to the other mail server](#).

Enter the target email address in the **Target email address** box. You can only specify one email address here

Enter the target SMTP mail server in the **Target email server** box. You can add username, password and alternate port numbers if you wish. The default is to connect on port 25 with no authentication. For example:

- *smtp.example.net* - will send the message to the server called 'smtp.example.net' on port 25, using no authentication
- *user:password@mail.example.com:587* - will send the message to the server called 'mail.example.com' on port 587, using the username 'user' and password 'password'.

Attempt to work with a single email address

When this option is chosen, VPOP3 tries to detect a user in the email comments associated with an email address

This option is not reliable and should not be used because it depends on too many external factors. It is only here for historical purposes from the early days of VPOP3, when email domains were expensive and many people did not have them. Nowadays, it is cheap to purchase a domain, and much more reliable.

Search subject line for a marker

When this option is chosen, VPOP3 tries to detect a user by looking for special text in the message subject

This option is not reliable and should not be used because it depends on too many external factors. It is only here for historical purposes from the early days of VPOP3, when email domains were expensive and many people did not have them. Nowadays, it is cheap to purchase a domain, and much more reliable.

5.4.2.2.3.1 Configure Routing Options

To get to this page, go to Mail Connectors → (choose Mail Collector) → [POP3 Routing](#) and press the **Configure Routing Options** button. This button is only available if the **Mail Collection Method** on the [General tab](#) is set to **Download from a POP3 Server**, and if the **Routing Method** is set to **Route by parsing message headers**.

Routing Options
close or Esc Key

Configure Routing Options

Close
Submit

Special Header Fields : ?

Used if your ISP provides extra routing information in non-standard message header fields.

Read Special Header Fields : Forwards ▼

Read "Received:" Header Fields : Reversed ▼

- Ignore "Resent-" header fields**
- Ignore Received: field recipients without an '@'**
- Ignore Standard (To: and Cc:) field recipients without an '@'**
- Disable default user -> user mappings**
- Ignore leading non-compliant "From" line added by some ISPs**

Header Processing Order

Special Headers ▼
Set Default

Stop Processing if any recipients found ▼
Check Order

Received: Headers ▼

Standard Headers (To, Cc etc) ▼

Stop Processing ▼

The **Special Header Fields** box lets you tell VPOP3 about custom header fields which your Internet provider may use to store recipient information in. VPOP3 will look in the standard (To, Cc, Received etc) header fields looking for recipients to try to recreate the [SMTP envelope](#), but some Internet providers add extra headers containing the actual SMTP envelope data which can make VPOP3 work better, for instance with BCCd messages.

Because these header fields are custom headers, there is no standard format for them, so the **Special Header Fields** box allows some complex entries to try to allow you to indicate which part of the header data it should use.

The simplest case is if the ISP adds something like *X-RCPTTO: user@example.com*. In this case, just add the line *X-RCPTTO* to the **Special Header Fields** box

In other cases, you can use a * symbol to indicate which part of the data VPOP3 should look at. For instance, if the ISP adds something like *X-Recipient: account-5123112 user@example.com delivered,*

you could add the line *X-Recipient: account-5123112 * delivered* to the **Special Header Fields** box. VPOP3 will then look for text preceded by 'account-5123112' and followed by 'delivered', and it will use the text in the middle as the recipient email address

Another option is if the ISP puts random text at the end of the line. In this case, you can use ~ to match the random text at the **end** of the line, after the email address. For instance *X-Recipient: abc * ~* will match *X-Recipient: abc user@example.com wumpus xyzzy*

Note that in all the above cases, VPOP3 will only match a single address per header line.

Starting in VPOP3 v6.7 you can also use regular expressions in the **Special Header Fields** box. To use these, surround the field data match text with / characters, and follow it with PERL-compatible match flags. You should use one or more captures (.) where you want VPOP3 to capture email addresses. Use the 'g' flag to indicate the match should be repeated. Some examples are:

- X-Recipient: /<([>@]+@[a-z0-9.-]+)>/ig
- X-Delivered: /^account-5123112 (.*) delivered/i

The **Read Special Header Fields** option lets you choose whether VPOP3 should start at the top of the message and work down to find the first matching Special Header field (*Forwards*), or start at the bottom of the headers and work upwards (*Reversed*) or find all matching Special Header fields (*All*).

The **Read "Received:" Header Fields** option lets you choose whether VPOP3 should start at the top of the message and work down to find the first matching Received: Header field (*Forwards*), or start at the bottom of the headers and work upwards (*Reversed*) or find all matching Received: fields (*All*).

The **Ignore "Resent-" header fields** option tells VPOP3 to ignore header fields such as **Resent-Cc**, **Resent-To** etc. Normally these header fields should be ignored, but some mail forwarding services add them so that the original recipients are listed in the Resent- header fields and the forward target is listed in the To header field. In this case you should turn this option off, so that VPOP3 will check the Resent- header fields to see who the message is for.

The **Ignore Received: field recipients without an '@'** option tells VPOP3 to ignore Received: headers where the 'for' clause recipient does not contain an @ symbol. Usually you will want to ignore these because they are rare and often have special meanings to the mail server if they exist, rather than being real email addresses.

The **Ignore Standard (To: and Cc:) field recipients without an '@'** option tells VPOP3 to ignore these recipients if their addresses do not contain @ symbols. Usually you will want to ignore these because the domain of the recipient is ambiguous and is more likely to refer to the sender's domain than your domain.

The **Disable default user -> user mappings** tells VPOP3 to ignore the implied Mapping of <username>@<accepted domains> to <username>. In most cases, these implied Mappings are useful shortcuts, but in a few cases (e.g. where you have multiple separate companies using the same mail server) then they may lead to ambiguities so you may wish to turn them off.

The **Ignore leading non-compliant "From" line added by some ISPs** option tells VPOP3 to ignore the invalid *From* line added by some ISPs to the top of messages. This usually happens if the ISP's mail server is buggy and is reading MBOX format files incorrectly. There is usually no reason to turn this option off. If this option is off, and the ISP does add a non-compliant *From* line, VPOP3 will take that to indicate the end of the message headers, and the message will not be processed correctly.

The **Header Processing Order** boxes let you tell VPOP3 in which order it should process the different type of header information. The default is

1. **Special Headers** - VPOP3 will find any recipients found by the **Special Header Field** matches.

2. **Stop Processing if any recipients found** - VPOP3 will stop processing header recipients if any valid recipients have been found so far
3. **Standard Headers** - VPOP3 will find any recipients listed in the To, Cc, Apparently-To header fields
4. **Stop Processing if any recipients found** - VPOP3 will stop processing header recipients if any valid recipients have been found so far
5. **Received: Headers** - VPOP3 will find any recipients listed in the Received header fields

5.4.2.2.4 Routing Errors

To get to this page, go to Mail Connectors → (choose Mail Collector) → Routing Errors. This tab is only available if the **Mail Collection Method** on the [General tab](#) is set to **Download from a POP3 Server** and the routing method set on the [POP3 Routing](#) tab is set to **Route by parsing message headers**.

This page tells VPOP3 what to do if it can't find any valid recipients after parsing the message headers to find the recipients.

The screenshot shows the 'Edit Mail Collector settings - MyISP (1)' page. The 'Routing Errors' tab is selected, showing the following options:

- Send an Error Message to Main Administrator (paul) (including the incoming message)
- Send the Incoming Message to Main Administrator (paul)
- Send an Error Message to:
- Send the Incoming Message to:
- Bounce to sender and don't keep local copy
- Ignore
- Send a bounce message to the sender

Don't generate bounce messages if spam score >=

Routing errors can occur if your ISP has a catch-all POP3 mailbox and someone sends a message to a non-existent user, or if someone sends a message to you using a [BCC](#), which means that the recipient email address will not be in the headers anywhere that VPOP3 can find it.

The main section is a choice of 6 options for what to do if there is an incoming message with no recognised recipients:

- **Send an error message to Main Administrator (<admin name>)** - this option makes VPOP3 send an error message to the [Main Administrator](#) indicating why the message could not be delivered automatically. The error message will contain the original incoming message as an attachment.
- **Send the incoming message to Main Administrator** - this option makes VPOP3 send the incoming message to the Main Administrator as if it was originally intended for them. This can look 'neater' than the above option because there isn't the extra error text, but it can make it harder to work out why the message couldn't be delivered properly, or can cause confusion because the administrator may think the message was actually addressed to them.
- **Send an Error Message to** - this is the same as the first option above, but the recipient is specified explicitly.

- **Send the incoming message to** - this is the same as the second option above, but the recipient is specified explicitly.
- **Bounce to sender and don't keep local copy** - a bounce message is sent to the message sender and the message is deleted. The bounce message can be customised using the **Customise Bounce Message** button below.
- **Ignore** - the message is simply discarded silently.

The **Send a bounce message to the sender** option will do the above option and also send a message to the original sender to tell them that the message could not be delivered. The bounce message can be customised using the **Customise Bounce Message** button.

Note that sending a bounce message in this way can cause something called *backscatter*. This happens because spammers can forge sender email addresses quite easily, so when you send a bounce message back, that bounce message is not going to the spammer but to some innocent person whose email address was forged by the spammer. Thus, it is generally considered bad manners to do this. Bounce messages sent as part of an [incoming SMTP transaction](#) are fine because those shouldn't cause backscatter because they work totally differently.

The **Don't generate bounce messages if spam score >= ...** - this tells VPOP3 not to generate a bounce message if the spam score is greater than the specified amount. This can help reduce the problem of backscatter.

5.4.2.2.5 Messages

To get to this page, to Mail Connectors → (choose Mail Collector) → Messages. This tab is only available if the **Mail Collection Method** on the [General tab](#) is set to **Download from a POP3 Server**.

Users Lists Mappings Mail Connectors Services Settings Status Reports About Help Search WebMail Logout

Connections
My Connection2
test2
Add New Connection

Mail Collectors
DRSmith
SMTP In
MyISP
Add New Collector
Import Collectors

Mail Senders
My Connection2
test2
Add New Sender

Newsgroups
Bob
Add New News Collector

Connector Schedule

Edit Mail Collector settings - MyISP (1) Show Hints

Delete Submit

General POP3 General POP3 Routing Routing Errors Messages

Messages

If you have told VPOP3 to leave messages on the ISP, you can tell VPOP3 to re-download some messages, or delete them from the ISP. These actions will take place on the next connection to the ISP. Note that it is possible that the messages listed below have already been deleted from the ISP by another program. Look at the 'Last Seen' column to see when VPOP3 last saw this message on the ISP's server.

If the message has not yet been downloaded from the ISP, then many of the columns will be blank because VPOP3 does not know that information yet.

Changes made to this table take effect immediately; you do not need to press the Submit button

Subject	Sender	Recipients	Message Date	Retr Date	Last Seen Date	Get	Del
						<input type="checkbox"/>	<input type="checkbox"/>

VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 Idle In: 46234 Out: 0

This page shows messages which VPOP3 believes are on the remote POP3 server. You can tell VPOP3 to delete them from the ISP the next time it connects or download them again if they have already been downloaded.

The table will show the subject, sender, recipients, message date, retrieval date and the date that VPOP3 last saw the message on the ISP.

If VPOP3 has not yet downloaded the message, then all except the 'last seen date' may be empty because VPOP3 only knows this information once it has downloaded the message. This means that if VPOP3 connects, sees there are 10 messages on the ISP and then the connection drops, this table will show 10 rows, each with no data except the 'last seen date'.

In the table, you can click the **Get** checkbox for a message to tell VPOP3 to retrieve it *if possible* the next time it connects (it's possible that the message has been deleted by the next time VPOP3 connects, so, in that case, VPOP3 can't possibly retrieve it).

You can click the **Del** checkbox for a message to tell VPOP3 to delete that message the next time it connects (assuming it hasn't already been deleted).

The **Get** and **Del** checkboxes in the message header will set the relevant checkbox for all messages in the table.

5.4.2.2.6 SMTP Options

To get to this page, go to Mail Connectors → (choose Mail Collector) → SMTP Options. This tab is only available if the **Mail Collection Method** on the [General tab](#) is set to **Incoming SMTP Feed**.

The screenshot shows the VPOP3 Enterprise 6.20 web interface. The top navigation bar includes links for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. The left sidebar shows a tree view of the configuration structure, including Connections, Mail Collectors, Mail Senders, and Newsgroups. The main content area is titled "Edit Mail Collector settings - SMTP In (5)" and has tabs for "General" and "SMTP Options". The "SMTP Options" tab is active, showing "Incoming SMTP Options".

Incoming SMTP Options

Incoming SMTP means that VPOP3 will receive email by messages being sent directly to VPOP3's SMTP service by a remote mail server. VPOP3 will actually always accept messages sent to it using SMTP. These settings are only needed if VPOP3 has to do something (such as dial a connection, or send an **ETRN** command to a remote server in order to trigger the remote server to start sending the messages).

If VPOP3 is dialing a connection for Incoming SMTP email, then VPOP3 has to wait a certain time for the incoming mail to start arriving. If it didn't wait, the remote mail server would have no time to start sending messages. If it waited until mail arrived, then it would stay online forever if no incoming mail was pending.

Once incoming mail starts arriving, VPOP3 will stay online until the remote mail server stops sending email.

Wait for up to : 20 seconds for an incoming SMTP connection

Some ISPs require you to send an **ETRN** command to trigger their mail server to start sending messages. If that is required, configure it below. You need to know the server to send the **ETRN** command to, and the parameters to send with the **ETRN** command (usually the email domain or user account name)

Use ETRN

Server to send ETRN to :

Parameters for ETRN :

Incoming SMTP uses the SMTP service to process incoming messages, so you can use [SMTP Rules](#) to filter incoming SMTP messages.

At the bottom of the page, the status bar shows: VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23 | Idle | In: 51425 | Out: 0

If you want VPOP3 to receive [incoming emails using SMTP](#), then normally you don't need to do anything. You normally *do not need* a Mail Collector for incoming SMTP.

Incoming SMTP mail usually arrives into an [SMTP Service](#) listening on port 25 (the standard SMTP port). As long as you have a VPOP3 SMTP Service listening on port 25 and your firewall allows incoming connections to port 25, then VPOP3 will receive incoming mail. You should make sure that VPOP3 is not configured as an 'open relay' so that it is not misused by spammers or other unauthorised people.

The only time you need to create a Mail Collector for incoming SMTP is if you need VPOP3 to actively do something. Your ISP will tell you if this is necessary. Nowadays it is rare because people usually have permanent Internet connections so incoming SMTP mail can arrive at any time, but in the days of dial-up connections often something needed to happen to tell your ISP to send ('dequeue') your waiting messages to you.

With POP3 collection, VPOP3 connects to a remote server, logs on and pulls down messages. With incoming SMTP nothing like this happens - it is a push system, so the remote server decides to send messages to VPOP3 whenever it feels like it.

If you have a permanent connection then messages arrive whenever they need to, so you don't need to do anything.

If you have an intermittent connection (eg dial-up) which supports SMTP then the messages are normally queued up at a server at your ISP which will wait until it decides to try sending them to you. In that case, often something will trigger the ISP's server to start sending them. This page supports two 'things' that VPOP3 can do to support common types of incoming SMTP mail on intermittent connections.

Waiting for incoming connections

With dial-up connections, sometimes the ISP's server will be triggered by the act of you actually dialing in. If nothing else happened, then VPOP3 would dial in, send any pending outgoing messages and then drop the connection. If there were no pending outgoing messages, it would dial in, then immediately drop the connection, possibly before the ISP could do anything.

So, the **Wait for up to X seconds for an incoming SMTP connection** option tells VPOP3 that after dialing up, it should wait at least the specified time before dropping the connection (if there are outgoing messages it might wait longer). If VPOP3 detects an incoming SMTP connection during this time it will stay connected to the dial-up connection until the incoming SMTP connection has ended and then drop the dial-up connection, even if the total online time is less than the time specified in this option.

So, if VPOP3 establishes a dial-up connection and is told to wait 30 seconds, but there is an incoming SMTP connection which starts after 3 seconds and lasts 5 seconds, VPOP3 will hang up 8 seconds after connecting (unless outgoing messages are still being sent).

This option is meaningless with permanent Internet connections.

Sending ETRN command

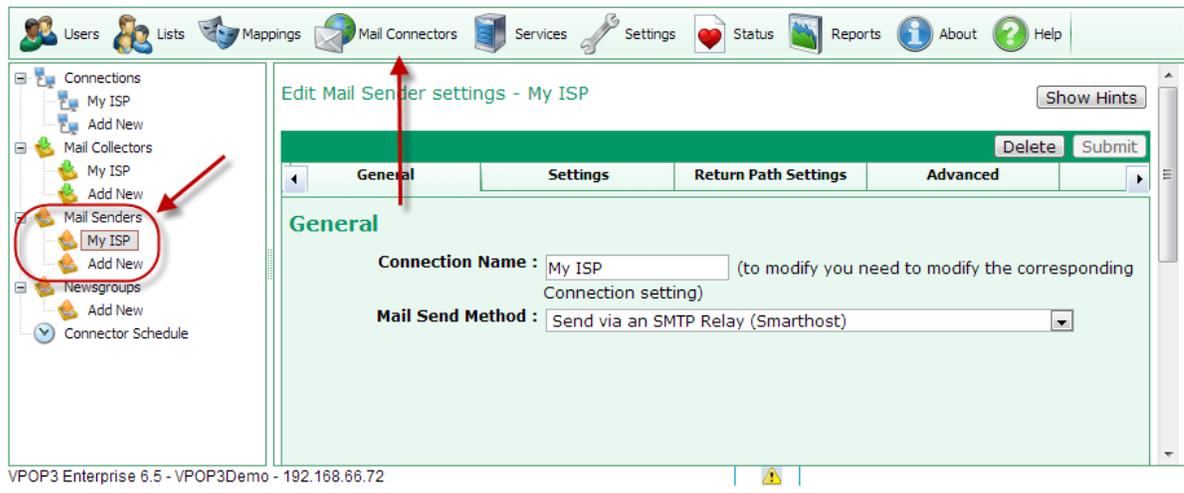
Some ISPs require you to send a command called '[ETRN](#)' (Extended Turn). This is a command which is sent to a remote server to tell a (potentially different) server to start sending messages to you. This was often used with dial-up Internet connections. It could still be used with permanent Internet connections but there is usually no need, so it is rarely used in that situation.

If your ISP requires you to use ETRN, they will explicitly tell you and will tell you the SMTP server you need to send the ETRN command to (**Server to send ETRN to** option) and some parameter to send in the ETRN command (**Parameters for ETRN** option) which is often your domain name, but could be something else - your ISP will tell you what to use.

There is a related SMTP command to ETRN called ATRN. The ATRN command is used in something called [On-Demand Mail Relay](#) (or ODMR). In VPOP3, you can set the Mail Collector type to ODMR to use this. One difference is that ETRN is usually used with static IP addresses and ATRN can be used with dynamic IP addresses. See the [ETRN & ATRN section](#) for technical details.

5.4.3 Mail Senders

In VPOP3 a [Mail Sender](#) tells VPOP3 how to send outgoing messages.



To access the **Mail Sender** settings, click on the **Mail Connectors** button on the top of the VPOP3 settings screen, then see the **Mail Senders** section of the tree on the left of the screen.

To [add a new Mail Sender](#), click on the **Add New** option under the **Mail Senders** section (note that this will add a **Connection** as well).

To [edit or view a Mail Sender](#), select the relevant **Mail Sender**, then look at the settings in the right-hand side of the screen.

To delete a **Mail Sender**, select the relevant **Mail Sender**, then click on the **Delete** button at the top-right of the **Mail Sender** settings.

5.4.3.1 Edit a Mail Sender

To edit a [Mail Sender](#), go to the VPOP3 settings, click on **Mail Connectors** at the top of the page, then select the appropriate **Mail Sender** from the [Mail Senders](#) section at the left of the page.

You will see 4 tabs which will vary depending on the type of **Mail Sender** you are viewing (see the **Mail Send Method**).

Send via an SMTP Relay

- [General](#)
- [Settings](#)
- [Return Path Settings](#)
- [Advanced](#)

Send using SMTP Direct

- [General](#)
- [Settings](#)
- [Return Path Settings](#)
- [Advanced](#)

5.4.3.1.1 General

Edit Mail Sender settings - My Connection2

Show Hints

Delete Submit

General Settings Relay Restrictions Return Path Settings Advanced

General

Connection Name : My Connection2
(to modify you need to modify the corresponding Connection setting)

Mail Send Method : Send via an SMTP Relay (Smarthost)

Last connection result : Connection successful

The **Sender » General** tab lets you set the basic options for a **Mail Sender** method. Note that in VPOP3, each **Mail Sender** is linked directly to a **Connection** method

The **Connection Name** is the name which you have given the **Connection** method which this **Mail Sender** is associated with. If you change the **Connection Name** here, it will also be changed for the associated **Connection**.

The **Mail Send Method** tells VPOP3 how VPOP3 will send outgoing messages. Most users will choose the **Send via an SMTP Relay** method, but advanced users may use the **Send using SMTP Direct** method.

The **Last Connection result** shows the result of the last time this Mail Sender was used by VPOP3.

Send via an SMTP Relay

This sending method is the way most people are most familiar with. Using this sending method, VPOP3 will send all outgoing messages to another SMTP server (often known as an *SMTP relay server*, or *Smarthost*). This other server is usually operated by your Internet provider. That other server then takes responsibility for delivering messages to the actual recipients' mail servers.

Advantages

- This method is simple.
- This method is the way most people are used to.
- This method is the way most likely to work.

Disadvantages

- There may be extra delays in sending.
- You are subject to any limitations your Internet provider may have in place, such as limits on the number of messages you can send at once, or the size of messages, etc.

Send using SMTP Direct

This sending method is the way that is actually used to send messages to the recipients' mail servers. If you send via your Internet provider's mail server, this is the method that your Internet provider's mail server will then send the messages out.

See the [SMTP MX Sending](#) topic for more technical details.

We generally recommend people use **SMTP Relay** sending, unless they are reasonably technical and are willing to put the extra effort in to get **SMTP Direct** sending to work reliably (the issues are not with VPOP3, but trying to persuade other people's mail servers to accept mail directly from your IP address).



Tip

If your Internet provider has imposed problematic limits on your mail sending, so you are considering using SMTP Direct to get around those limits, it can be worth considering asking your Internet provider if there is a way around their limits (they may have a 'business account' option with fewer limits), or using a third party SMTP relay service (we can [provide SMTP relay accounts](#) starting from £40+VAT per year, several other companies offer similar services).

Advantages

- The mail usually goes straight from your mail server to the recipients' mail servers, so you can see whether they have been delivered or not (messages will stay in [VPOP3's Outqueue](#) until the recipient's mail server has accepted them, or a delivery failure report is generated).
- There are no extra delays in sending.
- You are only subject to limitations of your VPOP3 server and the recipients' mail servers. Your Internet provider cannot impose extra limitations.

Disadvantages

- This method can confuse people, because messages may stay in the VPOP3 Outqueue for a while. This doesn't mean that VPOP3 is ignoring them, just that it has, so far, been unable to send them - for instance if the recipient's mail server is down.
- This method may not work, for instance, if the recipient's mail server doesn't trust your IP address. Many mail servers will look to see if the sending IP address looks to be on an ADSL/Cable connection, and, if so, will presume that that IP address should not have a mail server on it, so will block/discard your mail assuming that it is from a [spambot](#).
- This method may use a lot more bandwidth than sending via an SMTP relay server. If you send a 1MB message CC'd to 100 people, the upload will be about 1MB if using an SMTP relay server, but it could be up to 100MB (100 x 1MB) if using SMTP direct sending.

- This method can be more complex to manage and troubleshoot. If you are having trouble sending mail through your Internet provider's SMTP relay server, you can ask them to investigate. If you are using SMTP direct sending, then *you* have to do the investigation. This can involve having to read and understand the SMTP standards, doing DNS lookups, manually trying SMTP connections, etc.
- If your IP address gets blacklisted, you have to sort it out yourself, which can be time consuming.

5.4.3.1.2 Settings (SMTP Relay)

Edit Mail Sender settings - My Connection2 Show Hints

Changes have been made - press: Delete Submit

General	Settings	Relay Restrictions	Return Path Settings	Advanced
SMTP Relay Settings				
SMTP Relay Servers : (ISP's SMTP servers)		<input type="text" value="mail.isp.com"/>		
Session Encryption :		<input type="text" value="STARTTLS If Available"/>		
		<input type="checkbox"/> Log data for this sender		
SMTP Authentication				
		<input checked="" type="checkbox"/> This server requires SMTP authentication		
SMTP Username :		<input type="text" value="mycompany"/>		
SMTP Password :		<input type="password" value="....."/>		
Authentication Method :		<input type="text" value="Automatic"/> (Automatic is usually the best option, VPOP3 will pick the most secure method supported by your ISP).		

uk - 192.168.66.23 | Idle | In: 49259 | Out: 0

This **Sender » Settings** tab lets you set the options for a [Mail Sender](#) which is sending using [SMTP Relay](#) sending via another SMTP relay (Smarthost) server.

The **SMTP Relay Servers** box lets you enter the addresses of your Internet provider's SMTP relay servers (smarthosts). If you wish, you can enter more than one in this box - one per line. VPOP3 will attempt to connect to each server in turn until it finds one which responds, and then VPOP3 will send messages through that server. (Any SMTP errors reported by that server will *not* cause a subsequent server in this list to be tried).

VPOP3 will use TCP port 25 to connect to the SMTP relay servers, unless otherwise specified. To specify an alternate port, append a ':' (colon) to the server address, followed by the port number (with no spaces). For instance, to connect to *smtp.myisp.com* on port 587, you would use "smtp.myisp.com:587".

The **Session Encryption** option lets you specify whether any encryption of the connection between VPOP3 and the remote mail server should take place. There are four options:

- None - no encryption of the connection will take place.

- **SSL** - the connection will be encrypted as soon as it is established. This is a deprecated, non-standard, system, still used by some older mail servers. This will normally use an alternate port, often 465, although it is not standardised. This is sometimes known as *SMTPS*.
- **STARTTLS** - the connection will start off in plain text, and will switch to encrypted as soon as possible. This is the standard for SMTP session encryption. This will normally use the standard ports - 25 or 587. This is sometimes known as 'TLS'. If the remote server does not support STARTTLS encryption, VPOP3 will drop the connection and refuse to send messages.
- **STARTTLS if available** - the connection will start off in plain text, and will switch to encrypted as soon as possible if VPOP3 detects that the remote server supports STARTTLS. This will normally use the standard ports - 25 or 587. If the remote server does not support STARTTLS encryption, then VPOP3 will continue with the session in plain text. This option is usually the best option if you do not know whether or not the remote server supports encryption.

SMTP Authentication

The SMTP authentication options tell VPOP3 how to log in to your Internet provider's SMTP relay server to send messages.

Unlike [POP3](#) & [IMAP4](#), authentication in the [SMTP](#) standard is optional. Some Internet providers will not require authentication, instead only allowing access from IP addresses which are recognised.

If your Internet provider does require authentication, then check the **This server requires SMTP authentication** box, then in the **SMTP Username** and **SMTP Password** boxes, enter the relevant login details provided by your Internet provider (these are often the same as those used for collecting mail from the Internet provider).

The **Encryption Method** option lets you specify which authentication method VPOP3 will use for logging onto the remote server. Usually **Automatic** is the best option, as VPOP3 will pick the most secure method supported by both VPOP3 and the remote server.

VPOP3 supports two authentication methods:

- **Plain text** - the username & password are sent as plain text (if you look in the logs or monitor the TCP/IP traffic it may look encrypted, but it is a [Base64](#) encoding of the plain text, so is easy to convert back to plain text).
- **CRAM-MD5** - the username is sent in plain text, but the password is encrypted using a [challenge-response one way hash](#) encryption system. Using this system, the original password is hard to recover from the transmitted data, and it is virtually impossible to use a 'replay attack', so this is more secure than the plain text method. However, some mail servers report that they support CRAM-MD5 authentication, but their implementation is broken, so this may not work, and you may need to manually select the "Plain text" method.

Note that passwords are sent after any Session Encryption has been established, so if the session is encrypted, it is safe to use plain text passwords as the password will still be encrypted by the session encryption.

5.4.3.1.3 Relay Restrictions (SMTP Relay)

Edit Mail Sender settings - My Connection2 Show Hints

Changes have been made - press:

General	Settings	Relay Restrictions	Return Path Settings	Advanced
Remote Server Restrictions				
Max recipients per message : <input style="width: 100px;" type="text" value="999"/> (This is the maximum number of recipients per message that your ISP allows)				
Max recipients per session : <input style="width: 100px;" type="text" value="888"/> (This is the maximum number of recipients per session that your ISP allows)				
Max messages per session : <input style="width: 100px;" type="text" value="999"/> (This is the maximum number of messages that VPOP3 will send per session)				
Max messages : <input style="width: 50px;" type="text" value="0"/> per <input style="width: 50px;" type="text" value="0"/> minutes (0 to disable limit)				
Max recipients : <input style="width: 50px;" type="text" value="0"/> per <input style="width: 50px;" type="text" value="0"/> minutes (0 to disable limit)				

o.uk - 192.168.66.23 | Idle | In: 49259 | Out: 0

This **Sender » Relay Restrictions** tab lets you tell VPOP3 about any restrictions your ISP may have for sending messages.

The **Max Recipients per Message** setting tells VPOP3 how many recipients to specify per message that it sends out. . If you send a message to 100 people, and you have set this value to '15' to meet your Internet provider's requirements, then VPOP3 will send the message out 7 times, 6 times to 15 people each, and once to the remaining 10 people.

The **Max Recipients per Session** setting tells VPOP3 how many recipients are allowed in a single session connecting to the Internet provider's mail server. After this number of recipients has been reached, then VPOP3 will drop the session and not send any more messages until the next scheduled connection.

The **Max Messages per Session** setting tells VPOP3 how many messages are allowed in a single session connecting to the Internet provider's mail server. After this number of messages has been reached, then VPOP3 will drop the session and not send any more messages until the next scheduled connection.

The **Max messages: X per Y minutes** and **Max recipients: X per Y minutes** options let you set limits for how many messages or recipients can be sent in a particular time. So, for instance, if your ISP limits you to 1000 messages per hour, you could set **Max messages: 1000 per 60 minutes**. VPOP3 will simply not send any more messages after it has sent 1000 within 60 minutes, until some messages were sent over 60 minutes ago, then it will send more messages until it reaches the limit again. This will not allow you to bypass any limits placed by your ISP, but it will prevent error messages being generated and possibly messages being rejected and having to be resent.

5.4.3.1.4 Settings (SMTP Direct)

To get to this page, to Mail Connectors → (choose Mail Sender) → Settings (if the Sender uses the 'SMTP Direct' method).

This **Sender » Settings** tab lets you set the options for a **Mail Sender** which is sending using **SMTP Direct** sending directly to the recipients' designated mail servers.

When VPOP3 is sending using the "SMTP Direct" method, it has to determine where to send outgoing messages. It does this by querying the 'MX DNS records for the destination domain. So, it needs to access a DNS server to do this.

The **DNS Servers to use** box lets you specify DNS servers which VPOP3 should use. If you leave this blank, then VPOP3 will use the DNS servers configured in the Misc Settings. In some cases you may wish to specify different DNS servers here for reliability or other reasons.

The **DNS Overrides** button lets you specify **fake DNS entries** which VPOP3 will use in some cases. There are many uses for this facility, for instance:

- You may find that a particular recipient domain will not accept mail from you for some reason. In this case, you may wish to tell VPOP3 to use an SMTP relay server somewhere else (e.g. at your ISP) for sending to that domain.
- You can tell VPOP3 to send through a different mail server if it has failed to send messages for some time
- You can tell VPOP3 to send big messages through a different mail server
- You can tell VPOP3 to send messages from a particular user through a different mail server
- And so on.

VPOP3 remembers (caches) DNS results so it does not need to look up the DNS results again if it sends several message to the same domain. The **DNS cache size** setting tells VPOP3 the maximum number of cached results to keep. (It may keep fewer than this depending on how long the recipient specifies that DNS entries should be cached, and how often it sends messages).

The MX sending threads option tells VPOP3 how many messages it should send at the same time. Because VPOP3 may be sending each message to a different mail server, there can be some time while VPOP3 is negotiating the connection, so it helps performance if VPOP3 processes several messages at once. The default of 10 is a reasonable amount in most cases.

Remember that if you send a single message and list many recipients for that message in different domains, then, when using SMTP Direct sending, VPOP3 will have to send the message several times, once to each target domain.

5.4.3.1.4.1 DNS Overrides

To get to this page, to to Mail Connectors → (choose Mail Sender) → Settings (if the Sender uses the 'SMTP Direct' method) -> press **Edit DNS Overrides**

Edit SMTP Direct DNS Overrides

bob.com mail.psccs.co.uk

Enter the SMTP Direct Overrides in the box above. Each override should be on a line of its own, with the first part being the domain the override should apply to, and the second part being the name/address of the relevant mail server. For example:

aol.com smtp.myisp.com

You can use wildcards in the domain the override is applied to, eg *.domain.com - but note that in this example it would *not* match domain.com as well (because of the '.' after the *) so that would have to be added to the list separately.

If you need to specify authentication details, use **<username>: <password>@<server>**, eg **mycompany:mypassword@smtp.myisp.com** in the mail server portion.

When you send mail using SMTP Direct sending, VPOP3 usually determines which mail server messages should be sent to by looking at the message recipients and looking up the DNS 'MX' records for the recipient domain.

The DNS Overrides facility in VPOP3 lets you configure fake DNS MX records which VPOP3 should use instead of the ones defined by the recipient. This can be useful to alter how messages are sent.

VPOP3 will check all DNS Overrides which are specified. This may mean that there are multiple overrides for a particular message. In that case, VPOP3 will act as if there were multiple MX records set for the target domain. You can use the \$end operator (see below) to make VPOP3 stop if an override matches.

Basic DNS Overrides

Basic DNS overrides allow you to always route mail for certain domains through a particular server. This can be useful if SMTP Direct sending works most of the time, but some recipients reject it, so you want to send mail for those recipients' domains through an ISP SMTP relay server.

To do this, specify an override as

```
<target domain> <mail server to use>  
for example
```

```
example.com smtp.myisp.com
```

This means that VPOP3 will act as if the MX record for *example.com* is actually *smtp.myisp.com*, instead of the real MX record.

You can use wildcards in 'target domain' part, for example:

```
* smtp.myisp.com
```

will tell VPOP3 to send messages for any domain through 'smtp.myisp.com' (just as if you had told VPOP3 to send via an SMTP relay server)

If the specified SMTP relay server requires authentication, then you can specify that as:

```
<username>:<password>@<mailserver>  
for example
```

```
example.com joe:letmein@smtp.myisp.com
```

(Note that the ISP's SMTP server password is displayed in this case)

Also, you can specify the SMTP server port by adding :<port number> after the server name if it is not the default SMTP port of 25, for example

```
example.com smtp.myisp.com:587
```

Conditional DNS Overrides

As well as the basic overrides above, you can specify overrides which are conditional, depending on certain criteria, such as the message sender, size, how many times VPOP3 has tried to send the message already and so on.

To do this, specify the conditions after the basic override text. The conditions are specified as `<attribute><operator><value>`. There must be no spaces in the condition text. You can specify multiple conditions on a line. They must all match for the Override to be used.

Possible attributes to check are:

- `$retries` - this checks how many times VPOP3 has tried to send the message already. This may be useful if you want VPOP3 to try to send the message using MX sending originally, but send the message through an SMTP relay server if VPOP3 has tried several times without success.
- `$size` - this checks the message size. This may be useful if you want to send small or big messages through a particular server, and have other messages go direct.
- `$authsender` - this checks the authenticated sender the message was sent by (requires the sender to use SMTP authentication). This may be useful if you want VPOP3 to send messages from different users through different servers.
- `$from` - this checks the sender's email address. This may be useful if you want VPOP3 to send messages from different users through different servers and don't use SMTP authentication.

For all attributes, the following operators are available:

- `=` or `==` - test that the attribute value is equal to the condition's value
- `<>` or `!=` - test that the attribute value is not equal to the condition's value
- `<=` - test that the attribute value is less than or equal to the condition's value
- `<` - test that the attribute value is less than the condition's value
- `>=` - test that the attribute value is greater than or equal to the condition's value
- `>` - test that the attribute value is greater than the condition's value

For text attributes (`$authsender` & `$from`) the tests are case insensitive, and greater than/less than mean in terms of ASCII codes (`a < b`, `3 < a`, etc).

For text attributes only, the following two operators are also available:

- `~=` - test that the attribute value matches using [wildcards](#) or [regular expressions](#). Regular expressions are specified by surrounding the condition's value with `//` characters. For example `$from~="*@example.com"` will do a wildcard test, or `$from~/=/@example\.com/i` will do a regular expression test. Regular expression tests are case sensitive unless the 'i' flag is specified at the end.
- `~!` - test that the attribute value does not match using [wildcards](#) or [regular expressions](#).

Special conditions

There is a special override condition as well

`$dnsmx:<match>` - this makes the override match if any DNS MX records for the domain match the specified match text (using wildcard matches). For instance, you could use something like:

```
* smtp.myisp.com $dnsmx:*.aspmx.l.google.com $end
```

This will mean that mail to target email addresses using Google Apps will be sent via 'smtp.myisp.com' instead of direct.

You can precede the 'match' section with a '!' to change the meaning so that the override will match if *none* of the DNS MX records match the match text. For example:

```
* smtp.myisp.com $dnsmx:!*.example.com $end
```

More Override Options

- *\$end* - tells VPOP3 to stop checking the Overrides if the conditions on the current line matches. (If no conditions are specified, then the *\$end* option will always be used).
For example: * smtp.myisp.com \$authsender=joe \$end
- *\$adddns* - tells VPOP3 to use the normal DNS MX records as well as the override entries rather than replacing the DNS MX records by the overrides. This is not normally needed.
- *\$priority:<n>* - set the fake MX record priority to that specified. Not needed unless you use *\$adddns* or have several matching overrides for this particular recipient.

5.4.3.1.5 Return Path Settings

Edit Mail Sender settings - My ISP Show Hints

Delete Submit

General	Settings	Return Path Settings	Advanced
---------	----------	----------------------	----------

SMTP Return Path Modifiers

The SMTP Return Path is the address that bounce messages are sent to. Some ISPs also use it as a crude validation to see if the sender is allowed to use their SMTP relay server. By default VPOP3 will use the return path that the email client specifies, which is usually the email address of the sender. (Note for email which VPOP3 forwards on, the return path is the email address of the ORIGINAL sender in this case)

SMTP Return Path:

Change NULL return paths to : (leave blank to keep NULL return path - recommended)
 If you have to set this, because your ISP rejects NULL return paths contrary to the SMTP standard, make sure you specify a local address without an autoresponder or forwarding address.

The **Sender » Return Path Settings** tab lets you set any automatic modifiers for the SMTP return path when sending mail using this **Mail Sender**.

In [SMTP](#), the Return Path (or Return Address, or MAIL FROM address) is part of the SMTP envelope which is used to determine where bounce/delivery status messages will be sent. It is *not* the same as the 'Reply-to' address which is contained in the message header, and is where normal reply responses will be sent.

There are two modifications which VPOP3 can make to the Return Path

SMTP Return Path Modifiers

This option is most useful to deal with issues with forwarded messages. Normally if VPOP3 receives a message which it has to forward out itself, it will keep the original return path during forwarding. This can sometimes cause issues because:

- The original sender may be confused if they receive bounce messages for an email address they never used
- The Internet provider may reject the message because it appears to be from an address which is not one of their customers.

- An anti-forgery technology called [SPF \(Sender Policy Framework\)](#) may cause the messages to be rejected because they are coming from a mail server which is not approved by the return path's domain

The **SMTP Return Path** modifier has three options

- **Use default** - VPOP3 leaves the return path as it was originally. No changes
- **Always Set to:** - VPOP3 will always set the return path to the specified email address. The specified email address will receive all bounce messages & delivery status reports.
- **If the original address is not local, set to:** - VPOP3 will leave the return path as it is as long as it is a local email address. If the return path is not local, then VPOP3 will change it to be the specified email address. The original local users will receive bounce messages & delivery status reports for messages they send, but for forwarded messages, any such messages will be sent to the specified email address.

For problems with forwarding email, you would normally use the **If the original address is not local** option.

Remember that changing the return path using this setting will *not* change where any replies to the messages are sent.

Note that changing the return path in this way may not solve email forwarding problems if your Internet provider checks other things other than the SMTP return path - e.g. if they check the *From* or *Reply-To* header fields. In this case there is realistically nothing that VPOP3 can do to make forwarding work through your Internet provider's mail server. You may need to use a third party SMTP relay service, or have users [collect their mail directly from VPOP3](#), instead of using mail forwarding.

Null Return Paths

The **Change NULL return paths to** option lets you tell VPOP3 to use a specific return path address if it would otherwise use a blank return path.

In the SMTP standards, a blank return path is explicitly allowed, and has a specific meaning - which is to indicate that bounce messages should not be generated if a message cannot be delivered. This is extremely useful for automated messages, such as other bounce messages, or automated responses, because it prevents the creation of mail loops where two servers will endlessly send bounce messages between each other.

Unfortunately, some Internet providers have badly configured mail servers which prevent you using a blank return path. In this case, you can tell VPOP3 to change the return path to be a specific email address. The email address should be an email address on your domain which will *never* have any [forwarding](#) set, or any [autoresponders](#). For example, you could create a [distribution list](#) called '*no-reply*' with no members and set this setting to [no-reply@yourdomain.com](#).

If you do accidentally set VPOP3 to change null return paths to an email address with forwarding on, you could create a mail loop where messages are bounced between two servers endlessly. Changing this setting to a suitable email address instead should stop the loop from continuing.

5.4.3.1.6 Advanced

Edit Mail Sender settings - My Connection Show Hints

General Settings Relay Restrictions Return Path Settings **Advanced**

Advanced

Domain Filtering : 1 attempt: all

EHLO/HELO name :
(Leave blank to use default)

Only send messages waiting at start of connection
 Send smaller messages first (if this is not checked, VPOP3 will send messages on a "FIFO" basis)
 Reverse send order (ie largest messages first, or on a "LIFO" basis)

Sender Retry : minutes
This is the series of numbers telling VPOP3 when to retry messages. For instance **10,10,30,180** tells VPOP3 to retry a message after 10 minutes, then after another 10 minutes, then after a further 30 minutes, then every 3 hours until the 'Max Retry Time' (below) is reached.

Max Retry Time : hours
Warn after : hours

Timeouts

These settings apply to all mail senders

Initial banner: <input type="text" value="300"/>	HELO/EHLO response: <input type="text" value="60"/>	STARTTLS response: <input type="text" value="60"/>
AUTH response: <input type="text" value="60"/>	AUTH LOGIN response: <input type="text" value="60"/>	AUTH CRAMMD5 response: <input type="text" value="60"/>
ETRN response: <input type="text" value="60"/>	MAIL FROM response: <input type="text" value="300"/>	RCPT TO response: <input type="text" value="300"/>
DATA response: <input type="text" value="120"/>	END DATA response: <input type="text" value="600"/>	RSET response: <input type="text" value="60"/>
QUIT response: <input type="text" value="60"/>	ABORT: <input type="text" value="60"/>	

The **Sender » Advanced** tab lets you set advanced settings.

The **Domain Filtering** box lets you enter a set of rules to indicate whether a message which is waiting to be sent should be sent using this **Mail Sender** or not. For instance, this may be useful if you want to send mail from different domains or email addresses through different ISPs. It can be used for other things as well. Check the [Domain Filtering](#) article for more instructions.

The **EHLO/HELO name** is the name used by VPOP3 when it sends an EHLO or HELO command to a remote server. By default it uses the **VPOP3 Host Name** set in the [Settings » Misc Settings » General](#) tab, but you can customise it for a particular sender here.

If the **Only send messages waiting at start of connection** box is checked, then VPOP3 will only attempt to send the messages which were in the [Outgoing Queue](#) when the connection started. If this box is not checked, then when VPOP3 reaches the end of the connection it will perform another check to see if any more outgoing messages have arrived. If so, it will attempt to send those, then check again for any further messages, and so on.

If the **Send smaller messages first** box is checked, then VPOP3 will send smaller messages before bigger messages. If this box is not checked, then VPOP3 will send messages which arrived in the [Outgoing Queue](#) first.

If the **Reverse send order** box is checked, then VPOP3 will send messages which arrived in the Outgoing Queue more recently first (if the **Send smaller messages first** box is not checked), or bigger messages first (if the **Send smaller messages first** box is checked).

For the above two settings, note that outgoing messages can also have priorities assigned to them based on who sent the messages (configured in the User's [Advanced](#) settings tab). These priorities override any other ordering. Also, you can use [Lua scripting](#) to adjust sending priorities at runtime.

The **Sender Retry** box lets you specify when VPOP3 should try to send messages again, if previous attempts have failed. This is a list of time periods (in minutes) between try attempts. For instance, in the example shown (10, 10, 10, 30, 60, 60, 60, 180) this means that the second try will be 10 minutes after the first, then 10 minutes after that, then 10 minutes later again, then 30 minutes later, then an hour later, then another hour later, then another hour later, then three hours later. After that VPOP3 will try every three hours (the last number in the list is assumed to be repeated indefinitely). Note that these times do not override the [connection scheduling](#). If VPOP3's schedule is only set to send messages every hour, then there will be an hour between the first and second retries, and so on.

The **Max Retry Time** tells VPOP3 how long it should keep trying to send the message before failing it and sending a delivery failure message to the sender. The default is 72 hours which is usually the minimum recommended time (this allows for situations such as the recipient's mail servers failing on a Friday and not being fixed until the Monday).

The **Warn after** time tells VPOP3 that if a message has not been sent for this amount of time, then it will send a message to the original sender, telling them the message has not been sent yet, but it will keep on trying.

The **Timeouts** values set various times which VPOP3 will wait for responses from the remote mail server, depending on the state of the connection. The default values are taken from the relevant Internet standards where appropriate, so will normally not need to be changed.

5.4.3.1.6.1 Domain Filtering

The **Domain Filtering** box in a Mail Sender's **Advanced** tab lets you configure rules for whether VPOP3 should attempt to send a message through a Mail Sender, or whether it should skip the message. This can be useful if you need to use different Mail Senders for different things, such as messages from different users going through different ISP SMTP relay accounts.

This uses a very simple scripting language which will allow the most common conditions to be expressed simply. If you need more advanced conditions, then you may need to use [Lua scripting](#) which can do much more, because Lua is a fully featured programming language, but it is also more complex.

Domain Filtering Scripting Language

In the Domain Filtering scripting language, each line is either a rule or a comment. There are no variables, loops, or other programming structures.

Comments are lines which start with a # character and the comment continues to the end of the line. Comments are ignored by VPOP3.

Blank lines are allowed and are also ignored by VPOP3.

The script is case insensitive (except for regular expression comparisons).

Rule lines start with either **Attempt:** or **Skip:** which are then followed by one or more conditions

If the line begins with **Attempt:** then VPOP3 will attempt to send any message which matches *all* of the conditions specified on the remainder of the line.

If the line begins with **Skip:** then VPOP3 will skip any message which matches *all* of the conditions specified on the remainder of the line.

When VPOP3 finds an **Attempt:** or **Skip:** line which matches, it will stop processing the rest of the script.

If VPOP3 reaches the end of the script without finding a matching line, it will assume an **Attempt: All** if no other **Attempt:** lines were found in the script, or it will assume a **Skip: All** if any **Attempt:** lines were found. So, an empty script is equivalent to **Attempt: All**

The available conditions are:

All

This always matches

None

This never matches

Numeric comparisons

SIZE (comparator) (size)

This checks the size of the message to be sent.

The comparator can be <>, =, <=, >= (or == or != for people used to programming languages)

The size can just be a number, or a number followed by kB or MB. Numbers followed by kB are multiplied by 1024; numbers followed by MB are multiplied by 1048576 (1024 kB)

For example: **Skip: size > 50kB**

RETRIES (comparator) (number)

This checks the number of times the message has been attempted so far.

The comparator can be <>, =, <=, >= (or == or != for people used to programming languages)

For example: **attempt: retries >= 5**

AGE (comparator) (age)

This checks how long the message has been in the Outgoing message queue.

The comparator can be <>, =, <=, >= (or == or != for people used to programming languages)

The age is a number followed by **Minutes**, **Hours** or **Days** (the 's' on the end is optional)

For example: **Skip: age<10 minutes**

Text Comparisons

For text comparisons, the comparator can be <>, =, (or == or != for people used to programming languages), CONTAINS, MATCHES, REGEXP, NOT CONTAINS, NOT MATCHES or NOT REGEXP

For **MATCHES** comparisons, the text is some case insensitive wildcard text within quotes, for instance `"*@company.com"` or `"aa??@*.biz"`. This has to match the whole data (for a substring type match use `*` characters at the beginning and end).

For **REGEXP** comparisons, the text is a Perl compatible regular expression within `/ /` characters. These are case sensitive. If you want them to be case insensitive, put an `'i'` after the last `/` character.

For **CONTAINS** comparisons, the text is some text within quotes which needs to be contained within the data.

For `=` and `<>` comparisons, the text is some text within quotes which needs to match, or not match the data.

AUTHSENDER (comparator) (text)

This checks who sent the message (if they used authenticated SMTP).

For example: **Attempt: Authsender matches "and"**

Skip: Authsender = "bob"

FROM (comparator) (text)

This checks the email address which sent the message (the SMTP 'Return Path' value).

For example: **Attempt: From matches "@company.com"**

Attempt: from not contains "joe"

TO (comparator) (text)

This checks the email address the message is to (the SMTP recipient). Note that if the message is to several recipients, this can filter which recipients will be attempted and which will be skipped by this sender. If recipients are skipped, they will still be queued to be attempted by other senders.

For example: **attempt: to regexp /[abc]@company\.(org|com)\$/i**

Examples

Here are some simple examples of domain filtering rules.

Send all messages through this Sender except messages to example.com

```
skip: to matches "@example.com"
attempt: all
```

Send messages through this sender only if they are to example.com or example.org

```
attempt: to regexp /@example\.(org|com)$/i
skip: all
```

Send only messages from bob through this Sender

```
attempt: authsender = "bob"
skip: all
```

5.4.4 Connector Schedule

To get to this page, to Mail Connectors → Connector Schedule

Schedule Settings Show Hints

Schedule modifiers are configurable below the list of schedules.

Connection scheduling is currently active. [Click here to pause scheduling](#)

Enabled	Name	Connections	Description
<input checked="" type="checkbox"/>	Main Incoming3	Default	Every 10 minutes between 0:00 and 23:00 on Su,M,Tu,W,Th,F,Sa -
<input checked="" type="checkbox"/>	New Schedule2	My Connection2,tes	Once at 8:00 on M,Tu,W,Th,F if at least 1 message is waiting to be sent

If outgoing mail arrives whilst online, send immediately

Note that if you have **Connect Using LAN** selected on the **Connection** settings, VPOP3 will think that it is *always* online, so it will always send outgoing mail immediately if this option is enabled- this may be a problem if VPOP3 is connecting through a dial-up router or proxy server.

Send Immediately using these Connections: **My Connection2**
 test2

If no Connections are selected above, then VPOP3 will use the first suitable Connection.

If a connection occurred in the last : **minutes, don't check at the next scheduled time**

If at least : **people have checked their mail, connect within** **minutes.** (choose '0' people to disable this feature. This feature will connect using any 'Use with simple schedule' connections)

If a third party program changes the time, check if there's a scheduled connection required on the new time, rather than later than the new time (may cause duplicate connections at daylight savings change times)

VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 | Idle | In: 46220 | Out: 1

VPOP3 scheduling is quite flexible and you can create multiple schedules which work together to achieve greatness.

At the top of the page is a button where you can **Click here to pause scheduling**. This can be useful if you want VPOP3 to stop trying to send/receive messages due to a problem. Click the button again to resume scheduling.

Below that is a list of schedule configurations. You can create new schedules by pressing the **New** button, delete them by selecting them and pressing **Delete** or edit them by either clicking on the cells in the table (eg to disable or enable an individual schedule) or clicking the green text to edit the schedule details.

We recommend that you have at least one configured connection even if you may not think you need it (eg if you have VPOP3 sending outgoing mail immediately and have incoming SMTP) because the scheduled connections let VPOP3 download spamfilter & antivirus updates and check for important messages, etc.

Editing a schedule item

The screenshot shows a configuration window for a schedule item. At the top right are 'Submit' and 'Cancel' buttons. The 'Name' field contains 'Main Incoming3'. The 'Connect to' list has four options: 'Deny Connection' (unchecked), 'Default Connection(s)' (checked), 'My Connection2' (unchecked), and 'test2' (unchecked). The 'Connect' section has two radio buttons: 'Every 10 minutes' (selected) and 'Only once'. The 'Between these times' section shows '0 : 00' and '23 : 00' with a note '(times cannot span Midnight)'. Below this are two radio buttons: 'always' (selected) and 'If at least 0 messages are waiting to be sent'. The 'Connect on these days' section has checkboxes for all days of the week (Monday through Sunday), all of which are checked. To the right of the days are two buttons: 'Weekdays' and 'Every Day'.

The **Name** is just for your own reference.

The **Connect to** list lets you specify [Connections](#) which this schedule item will trigger. You can use **Deny Connection** to block connections - eg if you have one schedule set to connect every 5 minutes, you could create another schedule to **Deny** the connection every hour, so then it will connect at, say: 9:55, 10:05, and skip the 10:00 connection. The **Default Connection(s)** option tells VPOP3 to connect on all the Connections which have **Designate this connection a 'Default' connection** checked.

You can choose to have VPOP3 either **Connect every X minutes** between two specified times or just **Connect Only once** at a certain time.

Times *cannot span midnight*, so you can't have a schedule to connect between 21:00 and 09:00. Instead, you'd have to create two schedules, one to connect from 21:00 to 23:59, and one to connect from 0:00 to 9:00.

You can tell VPOP3 to **always** connect, or only to connect if there are a certain number of **messages waiting to be sent**. Note that the **messages waiting to be sent** counts the entire OutQueue size, not just messages that can be sent using the [Mail Senders](#) which this schedule item will trigger.

Then, you can tell VPOP3 which days of the week the schedule will apply to. The **Weekdays** and **Every Day** buttons are shortcuts to check the appropriate date boxes.

Extra Schedule Options

In the bottom half of the screen you can set further schedule options.

The **If outgoing mail arrives whilst online, send immediately** option tells VPOP3 to send outgoing mail immediately if either if it is currently connected through a dial-up connection, or if a selected connection is a **LAN** connection (through a router or proxy). VPOP3 won't wait for the next scheduled time to send the mail in this case. Note that even if you have this option set we recommend creating a schedule to handle retries if the first attempt to send a message fails.

Below this option you can specify connections to use for this 'send immediately' option in the **Send Immediately using these Connections** checkboxes.

The **If a connection occurred in the last X minutes, don't check at the next scheduled time** option lets you specify a limit for frequency of connections. For instance, if you have one schedule set to connect every 5 minutes, and one set to connect every 6 minutes, VPOP3 will connect at, say 9:05, 9:06, 9:10, 9:12, 9:15, 9:18 etc. If you set this option not to make a connection if one occurred within the last 2 minutes, VPOP3 will connect at: 9:05, 9:10, 9:15, 9:18 etc

The **If at least X people have checked their mail, connect within Y minutes** option lets you handle the situation where VPOP3 may not connect at evenings or weekends, but if people happen to be in the office, then it can still connect. This option was more useful with dial-up connections where connections cost money so disabling connections at quiet times was beneficial. With always-on connections it is not really useful.

The **If a third party program changes the time, check if there's a scheduled connection required on the new time** option is slightly complex. Normally at, say, daylight savings when the time changes, VPOP3 would schedule a connection for 2:00 am, then when the clock changes to 3:00am, VPOP3 will *not* schedule a new connection for 3:00am because it's still the same time as 2:00am was a moment earlier, so VPOP3 skips the new time when the clock changes and only checks for connections from a minute later. However, there are third party programs which keep resetting the clock (eg to keep track with an external time source). In that case, VPOP3 may never connect, because the time is being reset every minute. So, in that case, if you check this box, VPOP3 will check for connections *at* the new time, not just *after* the new time.

Advanced Scheduling

By judicious use of the multiple schedules you can do things such as make VPOP3 collect mail from some POP3 accounts more frequently than others.

For example, you could create two **Connections**, then create two **Schedules**, one to trigger each **Connection**. The first may trigger the first Connection every 5 minutes, and the second may trigger the second Connection every 30 minutes. Then, you could create several **Mail Collectors** and assign each to a **Connection** on the [General](#) tab as determined by how often you want that **Mail Collector** to trigger. VPOP3 will then trigger the **Connections** according to the schedules, and each **Connection** will start the appropriate **Mail Collectors**.

5.5 Services

VPOP3's **Services** are the services it offers to other software (usually email clients), such as POP3, SMTP, Webmail and IMAP4 (if you have VPOP3 Enterprise)

- [POP3 Server](#)
- [SMTP Server](#)
- [IMAP4 Server](#) (VPOP3 Enterprise Only)

- [Password Server](#)
- [Finger Server](#)
- [LDAP Server](#)
- [WebMail Server](#)
- [Status Server](#)
- [NNTP Server](#)

5.5.1 General

H:\devel\vpop3manual\screenshots\services_general_general.png

The Services -> General page lets you see an overview of the Services provided by VPOP3 and manage basic settings

- [General Tab](#)
- [Global Access Restrictions Tab](#)
- [SSL Settings Tab](#)

5.5.1.1 General

To get to this page, to to [Services](#) → [General](#) → General

The screenshot shows the 'Services' page in the VPOP3 administration interface. The 'General' tab is active, displaying a table of configured services. The table has the following data:

Type	Name	Enabled	Encryption	Binding
POP3	POP3 Server	<input checked="" type="checkbox"/>	None/STARTTLS	[Any IPv4] : 110
SMTP	SMTP Server	<input checked="" type="checkbox"/>	None/STARTTLS	[Any IPv4] : [Multiple Ports]
Password	Password Server	<input type="checkbox"/>	None	[Any IPv4] : 106
Finger	Finger Server	<input checked="" type="checkbox"/>	None	[Any IPv4] : 79
LDAP	LDAP Server	<input checked="" type="checkbox"/>	None	[Any IPv4] : 1389
WebMail	WebMail Server	<input checked="" type="checkbox"/>	SSL	[Any IPv4] : [Multiple Ports]
Status	Status Server	<input checked="" type="checkbox"/>	None	[Any IPv4] : 5109
IMAP4	IMAP4 Server	<input checked="" type="checkbox"/>	None/STARTTLS	[Any IPv4] : 143
NNTP	NNTP Server	<input checked="" type="checkbox"/>	None	[Multiple Addr] : [Multiple Ports]
SMTP	New SMTP Server	<input checked="" type="checkbox"/>	None/STARTTLS	[Any IPv4] : 5025
SMTP	SMTP Submission	<input checked="" type="checkbox"/>	None/STARTTLS	[Any IPv4] : 587
SMTP	New SMTP Server	<input checked="" type="checkbox"/>	None/STARTTLS	[Any] : 5026
SMTP	New SMTP Server	<input checked="" type="checkbox"/>	None/STARTTLS	[Any] : 5027
SMTP	New SMTP Server	<input checked="" type="checkbox"/>	None/STARTTLS	[Any] : 5028

Below the table, there is a 'Set Ports to Defaults' button and an 'Add Services' section. The 'Add Services' section contains the following text: 'You can add variants of the POP3 and SMTP service here. For instance, to bind to different ports, have different encryption settings etc.' and two buttons: 'Add POP3 Server' and 'Add SMTP Server'.

VPOP3 Enterprise 6.20 - lmail.pcs.co.uk - 192.168.66.23

Idle In: 49270 Out: 0

This page shows an overview of the services provided by VPOP3.

The table is editable. All the settings can be modified in the service settings themselves (on the **General** tabs) as well as here.

- Click the  icon to configure the service settings.
- If this is an additional service (in VPOP3 Enterprise only) you can click the  icon to delete the additional service.
- Double-click the name in the **Name** column to rename the service (this is for your reference only).
- Click the checkbox in the **Enabled** column to enable or disable the service. Note that the key services (POP3, SMTP & Webmail) cannot be disabled.
- Double-click in the **Encryption** column to alter the encryption type for the service if applicable (only in VPOP3 Enterprise, and only if an [SSL certificate has been installed](#)).
- Click in the **Binding** column to alter the IP address & port [bindings](#) for the service (which IP address(es) and port(s) the service will listen on). Note that in VPOP3 Basic a service can only listen on a single IP address/port option. In VPOP3 Enterprise it can listen on many different address/port options.

The **Set Ports to Defaults** button will set the standard service bindings to the default values (eg the POP3 service to listen on 'Any' address & port 110).

In [VPOP3 Enterprise](#) you can create multiple POP3 & SMTP services with different settings if you wish. Click the **Add POP3 Server** and **Add SMTP Server** buttons to add new services as appropriate. If you want to have the same settings on different TCP ports, then just use the **Binding** column; if you add extra services they can have totally different settings.

5.5.1.2 Global Access Restrictions

To get to this page, to to [Services](#) → [General](#) → Global Access Restrictions

The screenshot shows the VPOP3 web interface. The left sidebar contains a tree view of services including POP3 Server, SMTP Servers, IMAP4 Server, Password Server, Finger Server, LDAP Server, WebMail Server, Status Server, and NNTP Server. The main content area is titled 'Services' and has tabs for 'General', 'Global Access Restrictions', and 'SSL Settings'. The 'Global Access Restrictions' tab is active, showing the following text:

Global Access Restrictions

The global access restrictions apply to all services. If the global access restrictions are used for a service, then VPOP3 uses the most restrictive of the global access restrictions and the service specific ones.

VPOP3 will only use the global access restrictions if the service specific access restrictions are blank, **or** the server specific access restrictions have the "Use Global Address Restrictions" box checked.

Restrict	Type	Address	Prefix

Below the table are buttons for 'Add', 'Remove', and 'Defaults'. A 'Detected Network Info' section shows:

- Routers: 192.168.66.1, 192.168.66.1
- Networks: 127.0.0.0/8, 192.168.66.0/24, FE80::/64, ::1/128

A note at the bottom states: "(Note that the default settings might not be correct, especially if the VPOP3 server has a direct connection to the Internet. Check the settings before accepting them!)"

The status bar at the bottom shows: VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23 | Idle | In: 49273 | Out: 0

This page lets you set [access restrictions](#) which apply to all VPOP3's services. Access Restrictions limit which IP addresses can access the services.

In most cases this is left blank so that only the service-specific access restrictions apply, but if you add extra restrictions here, then they will apply in addition to the service-specific restrictions. A connection will have to pass *both* sets of access restrictions to be allowed. This can cause confusion when trying to add extra 'allow' restrictions because you may add an 'allow' restriction to the service-specific restrictions but it may still be denied by the global restrictions, so it won't work.

5.5.1.3 SSL Settings

To get to this page, to to [Services](#) → [General](#) → SSL Settings ([VPOP3 Enterprise only](#))

VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23

Idle In: 49274 Out: 0

This page lets you set the SSL settings used by VPOP3 when encrypting services. After making any changes to these settings **you must restart VPOP3** for them to take effect.

If you are not using a certificate with VPOP3, then this can be left blank, otherwise you will need to at least complete the **SSL Certificate Chain** and **SSL Private Key** boxes.

The **SSL Certificate Chain** box should contain the full SSL certificate chain in PEM format. The certificate chain contains all the certificates from the VPOP3 SSL certificate through to the one signed by the well-known certificate authority installed in your browser/email client. Usually whoever you obtained the certificate from should be able to provide this for you. The VPOP3 SSL certificate should be the first certificate in the list, followed by all the others in order.

The **SSL Private Key** box should contain the SSL private key you generated when generating the CSR to be signed by your certificate authority. Again, this should be in PEM format.

If you purchase an SSL certificate from us, we will send you the certificate chain & private key in the appropriate form, with instructions.

The rest of the options on this page are for advanced users only! VPOP3 uses OpenSSL so you can use the OpenSSL documentation to determine settings if necessary - eg the format of the **Allowed Ciphers** string is documented here: <https://www.openssl.org/docs/manmaster/apps/ciphers.html>

5.5.2 POP3

The VPOP3 POP3 service provides [POP3](#) services allowing local users to collect mail using a POP3 email client

- [General Tab](#)
- [IP Access Restrictions Tab](#)
- [Advanced Tab](#)

In VPOP3 Enterprise, you can create multiple POP3 services with different settings. To create multiple POP3 services, go to the [General](#) services page and press the **Add POP3 Server** button.

5.5.2.1 General

To get to this page, to to [Services](#) → [POP3 Server](#) → General

VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23

Idle | In: 45524 | Out: 0

Service Name is a name you have given to this POP3 server. It is most useful if you are using VPOP3 Enterprise and have [created multiple POP3 services](#). The name doesn't matter. It is used in the settings (in the service tree at the left of this page) and in any error messages, so that you can tell which POP3 service is being referred to.

The **Bindings** section is described in the [Service Bindings](#) topic.

The **Encryption** option is only available in VPOP3 Enterprise when an [SSL certificate is installed](#); VPOP3 Basic does not support encryption here. It can be **None/STLS**, **STLS** or **SSL**. POP3 supports two types of encryption, STLS and SSL.

STLS is the standard method. With this method, connections are usually made on the standard port (110). The server indicates to the POP3 client that encryption is available, and the client sends a **STLS** command to switch the session from plain text to the encrypted mode. No sensitive data (authentication details, message details, etc) is transmitted while the session is in plain text mode. **None/STLS** means that VPOP3 offers encryption to the client, but will allow unencrypted connections. **STLS** means that VPOP3 offers encryption to the client, and requires it to be used.

SSL is a deprecated method. With this method, the connection is made on a port other than port 110 (usually port 995) and starts off encrypted. This means that the POP3 client must know that the session is encrypted before it connects, otherwise it won't be able to establish a connection successfully.

Bandwidth Throttling allows you to set limits on how fast data will be transferred through this SMTP service. This allows you to prevent it taking up all your available bandwidth. See the [Bandwidth Throttling](#) topic for more information.

The **Log data for this service** option tells VPOP3 to log session data to a log file **POP3SVR.LOG** (see the [Diagnostics settings](#) for more information. It is equivalent to turning on 'Log POP3 Server Connections' on that page).

5.5.2.2 IP Access Restrictions

To get to this page, to to [Services](#) → [POP3 Server](#) → IP Access Restrictions

This tab is present for all VPOP3's Services. For general details on how this tab works, see the [IP Access Restrictions](#) section.

5.5.2.3 Advanced

To get to this page, to to [Services](#) → [POP3 Server](#) → Advanced

The screenshot shows the VPOP3 Enterprise 6.20 administration interface. The top navigation bar includes links for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, and WebMail. The left sidebar shows a tree view of services, with POP3 Server selected. The main content area is titled 'POP3 Service Configure' and has a 'Show Hints' button. Below the title is a 'Submit' button. The 'Advanced' tab is selected, showing 'Advanced Settings'. The settings include:

- Implement fix for Microsoft Internet Mail build 1160** (This option makes VPOP3 slightly modify messages as they are downloaded by removing extra blank lines from the end - these would cause Microsoft Internet Mail build 1160 to hang).
- Hold messages instead of deleting them** when processing the POP3 "DELE" command. This can be used as a crude backup facility on the server - this will probably use a LOT of disk space!

Below these settings is a field for 'Max failed login attempts : 3 per session (then connection drops)'. The status bar at the bottom shows 'VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23' and 'Idle | In: 45530 | Out: 0'.

The **Implement fix for Microsoft Internet Mail build 1160** option is to implement a workaround for a bug in a VERY old version of Microsoft's free email client (the precursor to Outlook Express). There is no harm leaving this option on, but it should equally cause no problems to turn it off nowadays because it is very unlikely that Microsoft Internet Mail is still being used (it was replaced by Outlook Express in 1997). This option removes blank lines from the end of the message.

The **Hold messages instead of deleting them** option tells VPOP3 that when the POP3 email client deletes a message, VPOP3 should 'hold' the message instead. Held messages are invisible to email clients so this will make the message appear to have been deleted as far as the email client can see, but it will still be present on the server. Note that there is no automated 'cleanup' option in VPOP3, so if you enable this option, the mailbox size in VPOP3 will grow indefinitely.

The **Max failed login attempts** option tells VPOP3 how many failed login attempts to allow in a single session before the connection is dropped and the client will have to reconnect.

5.5.3 SMTP

The VPOP3 SMTP service provides [SMTP](#) services allowing local users to send mail, as well as [incoming messages via SMTP](#) (if your firewall is configured appropriately and your domain MX records are set accordingly).

- [General Tab](#)
- [Filtering Tab](#)
- [Load Limiting Tab](#)
- [IP Access Restrictions Tab](#)
- [Spam Reduction Tab](#)
- [VRFY/EXPN Tab](#)
- [Advanced Tab](#)
- [IDS/IPS Tab](#)

In VPOP3 Enterprise, you can create multiple SMTP services with different settings. This would allow, for instance, you to create an SMTP service on port 25 for incoming mail, and an SMTP Submission service on port 587 for authenticated users to send outgoing mail. To create multiple SMTP services, go to the [General](#) services page and press the **Add SMTP Server** button.

5.5.3.1 General

To get to this page, to to [Services](#) → [SMTP Server](#) → General

The screenshot shows the 'SMTP Service Configure' page with the 'General' tab selected. The 'General Settings' section includes the following fields and options:

- Service Name:** SMTP Server
- Bindings:** A table with columns 'Address' and 'Port'. The entry is '[Any IPv4]' with port '25'. Below the table is an 'Edit Bindings' button with '(default port: 25)'.
- Encryption:** A dropdown menu set to 'None/STARTTLS'.
- Bandwidth Throttling:** A dropdown set to 'No Limit' and a text input for '10000000 bytes/second'.
- Authentication Options:**
 - Require SMTP Authentication**
 - Require "POP3 then SMTP" authentication. Timeout:** 5 minutes (the timeout is global, not per SMTP server)
 - Require encrypted authentication.** (This is not supported by all email clients, but means that passwords are sent to the VPOP3 SMTP service in an encrypted form rather than as plain text.)
 - Do not require SMTP authentication for internal/incoming mail** (this should always be used if you have incoming SMTP mail and have enabled one or both of the authentication options above)
- SMTP Anti-Relay Protection:** A dropdown menu set to 'Check Client IP Address (Recommended)'
- Maximum Message Size:** 50000000 bytes (0 = no limit)
- Reject unrecognised local recipients** (recommended, usually enabled)
- Log data for this service**

At the bottom of the page, the status bar shows: VPOP3 Enterprise 6.15 - lmail.pcs.co.uk - 192.168.66.70 | Idle | In: 32342 | Out: 0

Service Name is a name you have given to this SMTP server. It is most useful if you are using VPOP3 Enterprise and have [created multiple SMTP services](#). The name doesn't matter. It is used in the settings (in the service tree at the left of this page) and in any error messages, so that you can tell which SMTP service is being referred to.

The **Bindings** section is described in the [Service Bindings](#) topic.

The **Encryption** option is only available in VPOP3 Enterprise when an [SSL certificate is installed](#); VPOP3 Basic does not support encryption here. It can be **None/STARTTLS**, **STARTTLS** or **SSL**. SMTP supports two types of encryption, STARTTLS and SSL.

STARTTLS is the standard method. With this method, connections are usually made on the standard ports (25 or 587). The server indicates to the SMTP client that encryption is available, and the client sends a **STARTTLS** command to switch the session from plain text to the encrypted mode. No sensitive data (authentication details, message details, etc) is transmitted while the session is in plain text mode. **None/STARTTLS** means that VPOP3 offers encryption to the client, but will allow unencrypted connections. **STARTTLS** means that VPOP3 offers encryption to the client, and requires it to be used.

SSL is a deprecated method. With this method, the connection is made on a port other than port 25 (usually port 465) and starts off encrypted. This means that the SMTP client must know that the session is encrypted before it connects, otherwise it won't be able to establish a connection successfully.

If you are using the SMTP service for incoming SMTP on port 25, you should use the **None/STARTTLS** option. Some remote SMTP servers may not support encryption, so using **STARTTLS** will cause them to be unable to send you mail. Using **SSL** on port 25 is strongly discouraged.

If you are setting up an SMTP service on port 587 for SMTP Submission, then you should use the **STARTTLS** option to be standards compliant, but most email clients will work without encryption if you have a reason not to use it.

Bandwidth Throttling allows you to set limits on how fast data will be transferred through this SMTP service. This allows you to prevent it taking up all your available bandwidth. See the [Bandwidth Throttling](#) topic for more information.

The **Require SMTP Authentication** option tells VPOP3 that SMTP clients must log in using SMTP authentication before messages can be sent. This is usually a good idea as it allows VPOP3 to be configured to control/log users' activity. In some cases, email clients may not support SMTP authentication. In that case, you could turn this option off, but a better way may be to use the **Allow Unauth** option in the [IP Access Restrictions tab](#), to allow specific computers to send without authentication. If you want to allow remote users to send mail through VPOP3, or to restrict which users can send mail from certain IP addresses, then you *must* enable SMTP authentication (or POP3 then SMTP authentication).

The **Require POP3 then SMTP authentication** option tells VPOP3 to support a deprecated alternative to SMTP authentication. This option tracks which IP addresses have logged in using the POP3 protocol, and then allows those IP addresses to send mail for a few minutes after that POP3 login. This option is generally not required nowadays because most email clients support proper SMTP authentication, but it is present because people required authentication in the days before the SMTP authentication standard was designed.

If you have both **Require SMTP Authentication** and **Require POP3 then SMTP authentication** enabled, then VPOP3 requires one or the other, not both, in order to send mail.

The **Require encrypted authentication** option means that VPOP3 will not accept login details if the password was sent in plain text. This means it will accept an encrypted form such as CRAM-MD5 authentication, or any authentication over an encrypted connection. Any attempt to log in using a plain text authentication method over an unencrypted connection will cause VPOP3 to reject the login, even if the login details are correct. This is useful for preventing network snooping or certain man-in-the-middle attacks from being able to access users' login details.

The **Do not require SMTP authentication for internal/incoming mail** option tells VPOP3 that even if authentication is required (see above), then incoming/internal messages will be accepted without the session being authenticated first.

If you are using the SMTP service for incoming SMTP, then you *must* enable this option, because you can't give a VPOP3 username/password to everyone who might possibly send you messages.

The **SMTP Anti-Relay Protection** option lets you tell VPOP3 how to detect whether it is can be used for relaying outgoing mail. Generally the **Check Client IP Address** option is the correct one to use, unless you are *sure* it should be something else!

There are four options here:

- **No Checks** - VPOP3 will allow any computer which is allowed to connect (using the IP Access Restrictions) to send mail. This will not work for incoming SMTP mail, as you would have to give every computer access to connect so they can connect to send you your messages, but doing so would allow them to send outgoing mail, so VPOP3 will be an open-relay, which is a BAD THING.
- **Check from LAN** - VPOP3 will check that the connection is coming over the network adapter (not a dial-up adapter). This is generally not a very useful check nowadays (it was useful in the days when people used modems).
- **Check FROM address** - VPOP3 checks that the FROM address in the message being sent is a local address. This is easy to fake, so is generally not a useful check nowadays.

- **Check Client IP Address** - VPOP3 checks the sending computer's IP address against the IP Access Restrictions. If the IP address is allowed there, then the computer is allowed to send outgoing email. All other IP addresses are allowed to send incoming mail, but not outgoing mail.

The **Maximum Message Size** setting lets you tell VPOP3 how big the largest message to be sent should be. We recommend this shouldn't be over about 50MB (50000000 bytes). This is a hard limit, and other limits which can be set (eg in [SMTP Rules](#) or per-user settings) will be limited by this size as well. Note that if you send attachments, they will generally grow by about 33% when put into an email, so a 20MB attachment will increase in size to about 26.7MB when sent as an email. Also note that any SMTP servers outside of VPOP3 may have a lower limit than VPOP3, so you may still have problems sending large attachments even if VPOP3 allows it.

Reject unrecognised local recipients tells VPOP3 to give an SMTP 'reject' response when a message is sent to an unrecognised recipient. This is strongly recommended and is the default option. If you don't use this option you may encounter unwanted error messages as the VPOP3 administrator, and VPOP3 may generate "backscatter", which is a BAD THING.

The **Log data for this service** option tells VPOP3 to log session data to a log file **SMTPSVR.LOG** (see the [Diagnostics settings](#) for more information. It is equivalent to turning on 'Log SMTP Server Connections' on that page).

5.5.3.2 Filtering

To get to this page, to to [Services](#) → [SMTP Server](#) → Filtering



The screenshot shows the VPOP3 Admin Settings interface. The top navigation bar includes: Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, and Help. The left sidebar lists various server types: General, POP3 Server, SMTP Servers (with 'SMTP Server' selected), New SMTP Server, SMTP Submission, New SMTP Server, IMAP4 Server, Password Server, Finger Server, LDAP Server, WebMail Server, Status Server, and NNTP Server. The main content area is titled 'SMTP Service Configure' and has a 'Show Hints' button. Below the title is a 'Submit' button. A tabbed interface shows 'Filtering' selected, with other tabs for 'Load Limiting', 'IP Access Restrictions', and 'Spam Reduction'. The 'Filtering' section is titled 'SMTP Rules' and contains the text: 'SMTP Rules allow basic filtering and management of messages which VPOP3 receives using SMTP. This might be locally sent messages or incoming SMTP messages. VPOP3 has a different set of SMTP Rules for each SMTP Service.' Below this text is an 'Edit SMTP Rules' button. The 'Spam Filter' section has a checked checkbox for 'Enable Spam/Content filter on SMTP messages' and a 'Timeout' field set to '60' seconds.

The Filtering tab lets you specify filtering on incoming SMTP connections.

The **Edit SMTP Rules** button lets you view & edit [SMTP Rules](#) which apply to this SMTP service. SMTP Rules are filtering conditions which look at the incoming message and can perform actions such as redirecting, blocking or ignoring messages based on conditions you specify.

The **Enable Spam/Content filter on SMTP messages** option lets you enable or disable the VPOP3 spam filter. This setting applies to all the SMTP services defined in VPOP3, and is the same setting as the **Enable Spam/Content filter on SMTP messages** setting in the [Spam filter settings](#).

5.5.3.2.1 SMTP Rules

To get to this page, go to Services → SMTP Server → Filtering → Edit SMTP Rules

This page lets you configure rules for how VPOP3 processes messages it receives using SMTP (either from local senders or via an [incoming SMTP feed](#)).

Edit SMTP Rules for SMTP Server

Changes take effect immediately Close

Add Rule							
↓	Ⓐ Reject anything to [redacted]@psecs.com	Reject	All	1 condition(s)	Edit	Delete	
↑ ↓	Ⓡ Reject messages to spamblock	Reject	All	1 condition(s)	Edit	Delete	
↑ ↓	Ⓜ Accept anything from local	Accept	Any	2 condition(s)	Edit	Delete	
↑ ↓	Ⓜ Accept anything from D[redacted]es	Accept	Any	2 condition(s)	Edit	Delete	
↑ ↓	Ⓜ Accept mail from [redacted]	Accept	Any	4 condition(s)	Edit	Delete	
↑ ↓	ⓓ Redirect bounces to PAUL	Redirect	All	2 condition(s)	Edit	Delete	
↑ ↓	Ⓡ Reject messages to supportreply from outside PSCS	Reject	All	2 condition(s)	Edit	Delete	
↑ ↓	Ⓡ Reject	Reject	Any	1 condition(s)	Edit	Delete	
↑ ↓	ⓓ (No name)	Redirect	All	2 condition(s)	Edit	Delete	
↑ ↓	Ⓡ Accept anything from Paul to Spamcop	Accept	All	2 condition(s)	Edit	Delete	
↑	Ⓡ Reject VPOP3Announce Spam	Reject	All	2 condition(s)	Edit	Delete	

VPOP3 processes SMTP rules in order from top to bottom. When it finds a rule whose conditions match the incoming message, it will process the rule, and then stop processing any further messages (except where stated otherwise below in the **Action** descriptions). You can re-order the rules by clicking the up/down arrows to the left of the rule names.

The A/R/M/D icon before the function name indicates the Stage at which that rule is processed. See below for information on processing stages.

In [VPOP3 Enterprise](#), each SMTP Service has its own set of SMTP Rules. When you create a new SMTP Service, the new service is created with a copy of the first SMTP Service's SMTP Rules, but from then on they can be edited separately.

You can add a new rule by pressing the **Add Rule** button at the top of the page, delete a rule by pressing the **Delete** button to the right of the rule name, or edit the rule by pressing the **Edit** button to the right of the rule name. Changes to rules take effect immediately, so there is no **Submit** button; just press the **Close** button to close the editor.

When you add or edit a rule, the rule editor will be displayed as below

SMTP Rule x

Name:

Stage:

Action:

Condition match:

Conditions

<input type="text" value="mailfrom"/>	<input checked="" type="checkbox"/> not	<input type="text" value="ends with"/>	<input type="text" value="@pscs.co.uk"/>	<input type="button" value="Delete"/>
<input type="text" value="rcpt to"/>	<input type="checkbox"/> not	<input type="text" value="wildcard matches"/>	<input type="text" value="supportreply@pscs.co.uk"/>	<input type="button" value="Delete"/>

The **Name** box contains a name you specify for the rule. The name can be anything, but it is best to make it something meaningful to make the rules easier to maintain and to help when looking in log files.

The **Stage** box lets you specify the stage of the [SMTP transaction](#) when the rule will be processed. The default is **Auto** when VPOP3 will look at the conditions being checked to work out when a suitable time to process the rule is. A message transaction has three stages:

1. **MailFrom** - when the sender specifies the email address that the message is being sent from (the 'return path'). VPOP3 also knows authenticated sender details (if any), sender IP address, current date & time, and possibly message size at this point. It does not know who the message is for, or any message header data such as message subject.
2. **RcptTo** - when the sender specifies who the message is being sent to (the 'recipients'). VPOP3 knows all the data for the **MailFrom** stage, plus the current recipient, previously specified recipients and the number of recipients. VPOP3 processes the rule once for each recipient specified by the sender, not just once per message. Note that VPOP3 knows 'recipients' at this stage, it does not know whether the recipient was specified in the To, Cc or Bcc header. That is only discovered when VPOP3 has received the message headers in the Message Data stage.
3. **Message Data** - when the sender has sent the message to VPOP3. VPOP3 knows all the data for the RcptTo stage as well as the message size and message headers and the type of recipients.

The **Action** box lets you specify what happens when the rule conditions match. See the Action Descriptions section below for more details.

The **Redirect to** box lets you specify an email address which the message should be redirected to if the rule matches. This box is only present for **Redirect** actions. A similar **Copy to** box is displayed for **Copy** rules. You can specify multiple email addresses by separating them with commas. With VPOP3 Enterprise you can also specify a target folder for local targets by adding a space and the folder name after the username - eg *fred Customers*, *bob* will send it to the "inbox" for the user "bob" and the "Customers" folder for the user "fred".

For **Set Header** actions, there is a **Header Line** box where you can specify the header line to add.

For the **Block IP Address** action, there is a **Duration** box where you can specify how long to block the sender IP address for.

For the **Call Lua Function** action, there is a **Function Name** box where you can specify the Lua function name to call.

The **Condition match** box lets you specify whether all the conditions must match for the rule to be triggered, or only any one of the conditions must match.

Below this you specify the conditions for the rule. You can specify as many conditions as you want. Press the **Add Condition** button to add a new condition, and delete an existing condition by pressing the relevant **Delete** button. See the Condition Descriptions section below for more details.

Action Descriptions

- **Accept** - VPOP3 will accept the message as normal.
- **Reject** - VPOP3 will reject the message with a 5xx or 4xx response. If the conditions included any DayNow or TimeNow conditions, then VPOP3 will use a 4xx response to tell the sender to try again later, otherwise it will use a 5xx response to indicate that the message should not be retried. The reject response will say something like *550 5.7.1 Sender Prohibited (x)*, where 'x' indicates the number of the SMTP rule which matched to help the VPOP3 administrator diagnose what happened.
- **Redirect** - the message will not be delivered to the original recipient(s) but will be redirected to the recipients specified in the SMTP Rule.
- **Ignore** - the message will be ignored by VPOP3. The sender will think the message was delivered OK. The message will be 'blackholed'.
- **Copy** - the message will be delivered to the original recipient(s) and will also be copied to the recipients specified in the SMTP Rule.
- **Hold** - the message will be accepted by VPOP3, but will be 'held' by VPOP3 which means that only administrators can see the message, and it will not be sent out or delivered to the user's email client.
- **Reject and Disconnect** - VPOP3 will reject the message as with the **Reject** action, but the SMTP session will be dropped immediately as well.
- **Set Header and Continue** - VPOP3 will add a message header to the incoming message. VPOP3 will then continue to process further Download Rules. (Note that the header is modified AFTER the download rules have run, so you cannot check for the changed header in later download rules).
- **Set Header and Accept** - VPOP3 will add a message header to the incoming message and accept the message. VPOP3 will then not process further Download Rules.
- **If** - if this rule does not match, VPOP3 will not process any more rules until it encounters an **Else** or **EndIf** rule.
- **Else** - this type of rule cannot have any Conditions. It must be used after an **If** rule.
- **EndIf** - this type of rule cannot have any Conditions. It must be used after an **If** or **Else** rule.

- **Block IP Address** - VPOP3 will block the sender IP address for the specified time.
- **Call Lua Function** - VPOP3 will call the specified Lua function in the [SMTP Rule script](#) and use the result of that function as the SMTP rule result

Condition Descriptions

Conditions have 4 parts:

1. the type of condition
2. optional **Not** flag. If this is set, then the match operator is inverted (eg if the match operator is 'Contains', then if you check the **Not** box, the match condition becomes 'Does not contain')
3. match operator (eg Contains, Equals etc)
4. data

Condition Types

The condition type can be ANY message header field, as well as some special pseudo-headers.

Common header fields to check are **From**, **To**, **Subject** etc. Note that if VPOP3 is checking a message header field it does not process the header data, but uses the full data from the raw header. This means that if you check for "**From**" "**Equals**" "**bob@company.com**", it is actually unlikely to match messages from bob@company.com. This is because often the From header would actually say **From: Bob Wright <bob@company.com>**, so VPOP3 will be comparing **Bob Wright <bob@company.com>** to just **bob@company.com**, and they are not equal.

You can check multiple headers by separating them with commas - a common example would be **To,Cc** to check both the To and Cc header fields. If either header matches, then the condition matches.

The pseudo-headers supported by VPOP3 are:

- **Always** - if the data is '1' then the condition matches, if the data is '0' then the condition doesn't match. The actual message data is not checked at all.
- **TimeNow** - this checks if the time now is within the range specified by the condition data. You can specify times as hh:mm or just hh and indicate ranges by using the '-' character. Eg '9:00-17:00' will match if the current time is between 9.00 am and 5.00 pm inclusive or 9-17 will match if the current time is between 9.00am and 5.59 pm. If you do not specify a From time, then 0:00 is assumed. If you don't specify a To time, then 23:59 is assumed. VPOP3 uses the local time on the VPOP3 computer for time checks. The match operator is ignored.
- **DayNow** - this checks if the day of week now is specified in the condition data. Sunday is 1, Monday is 2 etc. So, **DayNow - 135** will match if the current day is Sunday, Tuesday or Thursday. The match operator is ignored.
- **IPAddress** - this checks the sender's IP address against the condition data.
- **MailFrom** - this checks the SMTP Return Path/Mail From value against the condition data.
- **AuthUser** - this checks the SMTP authenticated user (if any) against the condition data.
- **RcptTo** - this checks to see if the recipient specified in the condition data is in the SMTP recipients already specified for the message.
- **ThisRcptTo** - this checks to see if the recipient specified in the condition data matches the SMTP recipient currently being specified for the message.

- **RcptCount** - this checks the number of SMTP recipients specified for the message.
- **Bcc** - this checks to see if the condition data matches any of the BCC recipients for the message. VPOP3 determines if a recipient is a Bcc recipient by comparing the SMTP recipients against those specified in the To and Cc header fields. Any SMTP recipient which is not listed in the header is assumed to be a Bcc recipient.
- **BccCount** - this checks the number of BCC recipients specified for the message.
- **Size** - this checks to see if the message size matches the condition data as indicated by the match operator.

Match Operators

All matches apart from regex matches are case insensitive. Numeric data is checked numerically for numeric operators like **greater than** etc. If you check numeric data with **contains**, **begins with**, **regex** etc, then the numeric data is converted to a string a tested as text.

- **equals** - the value matches the condition data exactly.
- **is** - the same as **equals**
- **not equals** - the value does not match the condition data.
- **greater than** - the value is greater than the condition data (text data is compared alphabetically).
- **greater or equal** - the value is greater than or equal to the condition data (text data is compared alphabetically).
- **less than** - the value is less than the condition data (text data is compared alphabetically).
- **less or equal** - the value is less than or equal to the condition data (text data is compared alphabetically).
- **contains** - the value contains the condition data as a substring.
- **wildcard matches** - the value matches the condition data when processed as a wildcard string (* and ? wildcards).
- **begins with** - the value begins with the condition data.
- **ends with** - the value ends with the condition data.
- **regex matches** - the value matches the specified regular expression - specified as `/<regex>/<flags>` - eg `/my cat/i`

Diagnostics

VPOP3 creates a log file in the [log path](#) called **SMTPRULES.LOG**. This log file contains information on all download rules which are triggered.

If the message is rejected by the SMTP rules, the rejection text will contain the rule number in parentheses. Possible SMTP rejection lines are:

- 450 4.7.1 Recipient Prohibited
- 450 4.7.1 Sender Prohibited
- 454 4.7.1 Message Prohibited
- 550 5.7.1 Recipient Prohibited
- 550 5.7.1 Sender Prohibited

- 554 5.7.1 Message Prohibited

5.5.3.3 Load Limiting

To get to this page, to to [Services](#) → [SMTP Server](#) → Load Limiting

The screenshot shows the 'SMTP Service Configure' interface with the 'Load Limiting' tab selected. The settings are as follows:

- Maximum Incoming Sessions:** 50
- Maximum messages per incoming session:** 5 (0 = unlimited)
- Maximum messages per local session:** 2 (0 = unlimited)
- Maximum recipients per incoming message:** 3 (0 = unlimited)
- Maximum recipients per local message:** 2 (0 = unlimited)
- Maximum Incoming Sessions per client:** 10 (0 = unlimited)
- Reserve Sessions for:** 192.168.1.10, 192.168.1.11
- Number of Sessions to Reserve:** 30
- Send SMTP Keep Alive response every:** 0 seconds (0=disable. Using SMTP "keep alive" may cause interoperability issues)

At the bottom of the window, the status bar shows: VPOP3 Enterprise 6.15 - lmail.pscs.co.uk - 192.168.66.70 | Idle | In: 29506 | Out: 2

VPOP3 accepts multiple SMTP connections at once. Especially if you allow access from outside your network, this has the potential to allow remote computers to perform a Denial Of Service (DOS) attack on VPOP3, because it can be forced to process lots of messages at once. The **Load Limiting** settings for the SMTP service allow you to restrict how many SMTP connections VPOP3 will handle at once. Excess connections are refused with an SMTP error indicating the sender should try again later. For incoming mail this should not cause a problem because legitimate senders will be prepared for this type of behaviour so will simply queue the message and try sending it again a few minutes later.

It can be tempting to increase these limits, but doing so can be counterproductive. Increasing the limits too far will cause VPOP3 to process messages slowly, which may mean that the message sender times out and retries the message later. In this case, VPOP3 will still continue to process the original message, so now VPOP3 has to process that message twice (or more times) increasing the server load further, slowing things down further, meaning more senders time out, and so on.

The **Maximum Incoming Sessions** setting tells VPOP3 how many incoming connections it should allow. At connection time VPOP3 determines whether a connection is local or not from the [IP Access Restrictions](#) - any IP address which is allowed to send anonymously (with **Allow Unauth** enabled) is considered to be a local address. Some of these allowed sessions may be *reserved* for specific IP addresses - see below. So, the number available to arbitrary senders is the **Maximum Incoming Sessions - Number of Sessions to Reserve**.

For the next four settings, VPOP3 decides whether the connection is local or not depending on whether the IP address is allowed to send outgoing messages, so if the IP address is allowed to send

anonymously or the user has authenticated, then the session is a local session not an incoming session.

The **Maximum messages per incoming session** setting tells VPOP3 how many messages are allowed in a single incoming connection. Usually this would be quite small, because a particular sender shouldn't send many messages to you, but if your incoming mail arrives via a third party SMTP relay server, you may want to increase this number.

The **Maximum messages per local session** setting tells VPOP3 how many messages are allowed in a single local session. Usually this would be quite small because users will generally only send one or two messages at once. If you have an automated program which sends lots of messages in a single session, you may want to increase this number.

The **Maximum recipients per incoming message** setting tells VPOP3 how many recipients are allowed in a single incoming message. This is the number of RCPT TO commands, so if an incoming message is to a VPOP3 list, that will only count as one recipient, even though there may be many final recipients.

The **Maximum recipients per local message** setting tells VPOP3 how many recipients are allowed in a single locally sent message.

The **Maximum Incoming Sessions per client** setting tells VPOP3 how many connections are allowed from a single IP address. Usually this will be a small number to try to prevent a single remote computer from taking up all the available connections. If your incoming mail arrives via a third party SMTP relay server, you may want to increase this number. In this case whether a connection is local or not is the same as for the **Maximum Incoming Sessions** setting.

The **Reserve Sessions for** and **Number of Sessions to Reserve** options let you specify that a number of the available incoming sessions are reserved for particular IP addresses. So, in the example above, 50 incoming sessions are allowed. 20 of those are for arbitrary IP addresses, and 30 are reserved for the IP addresses 192.168.1.10 and 192.168.1.11. There is no way to reserve one quantity to one IP address and a different quantity to a different IP address, the reserved connections go into a 'pool' which can be used by any of the specified IP addresses. * and ? wildcards are allowed in the **Reserve Sessions for** setting - eg *192.168.1.** would reserve connections for any IP addresses in the 192.168.1.0/24 network.

The **Send SMTP Keep Alive response every x seconds** is an option to tell VPOP3 to send interim SMTP responses every few seconds to the message sender while a message is being processed. This can prevent the sender timing out the connection, but is not recommended because it can cause interoperability problems. Firstly, some mail sender do not support interim SMTP responses after message content has been sent, and secondly the way this option does things does not strictly conform to the SMTP standards (it is allowed to send interim SMTP responses, but the response code should be the same as the final response, and because VPOP3 does not know the final response the interim responses may have a different response code - most email senders seem to use the last response code meaning it works OK, but this may not always be the case).

5.5.3.4 IP Access Restrictions

To get to this page, to to [Services](#) → [SMTP Server](#) → IP Access Restrictions

This tab is present for all VPOP3's Services. For general details on how this tab works, see the [IP Access Restrictions](#) section.

For the SMTP Service, this page has several modes depending on other settings, the different modes look slightly different. The most common is below:

VPOP3 Enterprise 6.15 - I-mail.pscs.co.uk - 192.168.66.70

There are two things which can change depending on the mode:

Relay or connection restrictions

The text at the top will either say it defines computers *which are allowed to relay outgoing mail through this SMTP service*, or *computers which are allowed to connect to this SMTP service*.

On the **General** tab, if the **SMTP Anti-Relay Protection** is set to **Check Client IP Address**, then this tab defines which computers can relay outgoing mail through this SMTP service. Any other IP address can connect and send incoming/internal mail, but not outgoing mail.

If the **SMTP Anti-Relay Protection** is set to any other option, then this tab defines which computers can connect to the SMTP service at all. Allowed IP addresses can send both incoming/internal and outgoing messages. No other IP address can connect at all, either to send incoming/internal or outgoing mail.

We recommend the **SMTP Anti-Relay Protection** is set to **Check Client IP Address** in most cases. If your incoming mail arrives via a third party SMTP service, then you may wish to change the setting to **No Checks** and use the IP Access Restrictions to only allow local computers and the third party SMTP service to connect to the server (this method can *not* be used if you want to allow remote users to access VPOP3 using this SMTP service).

Users/Authentication

On the **General** tab, if **Require SMTP Authentication** and/or **Require POP3 then SMTP authentication** are checked, then the table will have **Allow Unauth** and **Users** columns. If neither of

those General-tab options are checked, then those two columns will not be present. That is because if SMTP authentication is not being used, then VPOP3 will not know which user is connecting, so there is no way for it to restrict access based on the user.

5.5.3.5 Spam Reduction

To get to this page, to to [Services](#) → [SMTP Server](#) → Spam Reduction

The screenshot shows the 'SMTP Service Configure' window with the 'Spam Reduction' tab selected. The settings are as follows:

- DKIM Signing:** Off
- DKIM Selector:** (empty)
- DomainKey Signing:** Off
- DomainKey Selector:** key1
- DomainKey/DKIM Keys on Server:**

Domain	Selector
pscs.co.uk	key1

To add more keys, save the private keys in the main VPOP3 installation directory as `domainkey_<domainname>_<selector>.key` - eg `domainkey_company.com_sel.key`.
- Greylisting:**
 - Enable Greylisting
 - Skip Greylisting if SPF check passes
 - ...with one of these SPF domains: (empty)
- Realtime Blacklist Rules:**
 - Realtime Blacklist Rules work with incoming SMTP mail to allow VPOP3 to check various online databases to see if the sending computer is listed as an open relay which is abused by spammers or is a specific mail server used by spammers.
 - [Edit Realtime Blacklist Rules](#)
- SPF:**
 - Enable SPF Support
 - Skip SPF checks for local/authorised senders
 - [SPF Whitelist](#)
 - Reject message if SPF check result is: Fail, PermError or TempError

DKIM & DomainKeys

The first part of this tab indicates whether the VPOP3 SMTP Service should digitally sign sent messages using the DKIM and/or DomainKeys systems.

DKIM is the current standard. DomainKeys was a previous system so should probably not be enabled unless you specifically need it. (It won't cause any interoperability problems, but it is probably pointless).

DKIM (and DomainKeys) add a digital signature to the message header which the recipient can use to check that the message has not been altered since it was sent. This will typically sign the message contents and important headers such as Subject, From, Date, etc.

Note that if the message passes through any other software which may modify the message after it has been signed by VPOP3, then that may cause the digital signature to fail, which may mean your messages are rejected. The type of software which may do this are some viruses scanners (which may add a 'scanned by XYZ Antivirus' line to the bottom of the message, for instance) or mailing list distribution software.

To use DKIM (or DomainKeys) you first need to generate a DKIM key pair. You publish the public key in your DNS, and put the private key in a PEM file in the VPOP3 installation directory called 'domainkey_<domainname>_<selector>.key'.

For instance, if you are sending mail from 'example.com' and have chosen the selector 'key1', you would save the private key in a file in the VPOP3 directory called 'domainkey_example.com_key1.key'.

The 'selector' is just a simple name you choose, which allows you to change the key without invalidating previously signed messages. If you change the key, you will choose a new selector, tell VPOP3 to use that, and leave the old selector's DNS entries online for a while so that messages in transit will still be able to validate using the old selector.

There are lots of resources online about DKIM key generation. If you search for 'DKIM key generator' you should find web pages that will generate the public & private keys in PEM format and tell you how to publish the public key in your DNS server.

When people send messages through VPOP3 it will look for a KEY file for the appropriate domain of the sender and use that. If such a file doesn't exist, then the message won't be signed.

Greylisting

Greylisting is an anti-spam technique where the server (VPOP3) temporarily rejects incoming SMTP messages. Legitimate mail servers will handle this seamlessly and will retry sending the message again later. VPOP3 will remember that the same mail server has tried to send the same message earlier, so it will accept the message the second time and remember the sending server is OK. Much software which sends spam will *not* retry the message, so the spam will disappear, so this simple technique can help to reduce spam quantities. It will lead to a short delay the first time someone sends a message to you, but it will not delay regular correspondence.

The [Wikipedia article on Greylisting](#) has more details on the process.

One of the problems with Greylisting is that it requires the same server as originally tried to send the message to be the server which retries the message later. In the vast majority of cases this is what happens, but some mail services have large farms of mail servers and don't manage them so that the same server handles the retries. This means that it may be a different server which tries to send the message the second time. VPOP3 will again delay that, because it sees it as a new message, and so on. Google's mail service is one of the prime examples of this. The **Customise Greylisting** option lets you configure IP addresses or sending domains which will not be Greylisted.

Starting in VPOP3 v6.20 there is another option which may be useful - the **Skip Greylisting if SPF check passes** option. If this is checked, then if the SPF check (see below) results in a Pass, then the Greylisting will be skipped. This is usually OK because the main spam sources which will be defeated by Greylisting are 'spam bots' which will not usually pass SPF checks.

If you want, you can specify text in the **...with one of these SPF domains** box. Each line will be compared with the domain name for the SPF check which passed. If it matches then Greylisting will be skipped, but other SPF passes will still trigger Greylisting (if the box is left blank then all SPF passes will skip Greylisting). For instance, domains which use Google Apps should use the SPF domain **_spf.google.com**, so if you put "_spf.google.com" in the text box anyone using Google Apps with a correctly configured domain should skip Greylisting.

The **...with one of these SPF domains** box needs each domain entry to be on a line of its own, and * & ? wildcards are allowed.

Realtime Blacklist Rules

Realtime blacklists are databases which use DNS to identify 'bad' IP addresses which send mail. VPOP3 will query the blacklists whenever an incoming SMTP connection occurs to decide if it should accept mail from that IP address. There are many, many different blacklists. You can use the [Edit Realtime Blacklist Rules](#) button to edit which blacklists VPOP3 uses. We don't recommend that you use a lot of blacklists or it can slow things down too much.

SPF

SPF (Sender Policy Framework) is a way of publishing in your domain's DNS records which IP addresses are allowed to send mail from your domain. This can be used to help the recipient know that the message really came from the sender it claims to have been sent from.

It is normally trivial for an email sender to pretend to be someone else, which can cause security problems if a malicious person pretends to send messages from your bank or manager. It can also cause problems with 'backscatter' or your company's reputation if they send spam using your email address as the sender. SPF allows the recipient to check that the message came from an 'authorised' mail server.

SPF records are set in your DNS, not in VPOP3. There are websites which will help you configure your SPF record. If you send mail through an ISP's mail server, then your ISP should be able to tell you which SPF record to use.

You should not have VPOP3 performing SPF checks on incoming mail if you receive incoming mail but it comes via another company's mail server (eg your ISP or a mail filtering company) because that will cause all the SPF checks to fail. Instead that other mail server should perform the SPF checks and react accordingly.

The [SPF Whitelist](#) allows you to bypass the SPF checks for known senders who have their SPF record configured incorrectly.

An SPF check will result in several different possibilities:

- None - there is no SPF record defined for the sending domain
- Pass - the SPF record indicates that the sending IP address is allowed to send from this domain.
- Fail - the SPF record indicates that the sending IP address is not allowed to send from this domain.
- Neutral - the SPF record doesn't indicate whether the sending IP address is good or bad. Often this is used when testing SPF.
- SoftFail - this is between Fail and Neutral. Often this is used when testing SPF. The message should be accepted but may be treated as more suspicious by a spam filter.
- TempError - this is usually caused by a DNS error at the recipient or sender end
- PermError - this is usually caused by a configuration error in the SPF record (eg invalid commands)

Reject message if SPF check result is

Starting in VPOP3 v6.20 you can tell VPOP3 to immediately reject messages if the SPF check fails in some way.

VPOP3 can be configured to reject different sets of results. It is not recommended that you reject SoftFail results, but this option is available if you wish.

TempError results will be rejected with a temporary error, telling the sender to try again later.

The **None** option means that VPOP3 will never reject mail based on SPF checks.

Also, if you are using the VPOP3 Spamfilter, there are various 'SPF' [spam filter rules](#) which can lead to mail being quarantined if it fails SPF checks.

5.5.3.5.1 Edit Realtime Blacklist Rules

To get to this page, to to [Services](#) → [SMTP Server](#) → [Spam Reduction](#) and press the **Edit Realtime Blacklist Rules** button.

Note that this option is only available in [VPOP3 Enterprise](#).

VPOP3 - Edit RBL Rules
Help Show Hints

Close
Submit

RBL Servers to use :
(one entry per line)

zen.spamhaus.org(127\,0\,0\,3)

"Blackhole" (throw away) blacklisted mail (not recommended)
 Accept blacklisted mail, but add a marker header line for filtering in your email clients.
 Reject blacklisted mail - the sender should get a delivery failure report.
 Redirect blacklisted mail To

Don't check IP addresses listed in the SMTP server access restrictions as "NOAUTH" for RBL entries.

IP address whitelist:
(one entry per line)

192.168.*
 10.*
 172.16.*
 127.*

Realtime Blacklists

[Realtime Blacklists \(RBLs\)](#) are DNS-based databases which contain lists of IP addresses known to be used for sending spam, or known to be compromised with 'bots' or which are not meant to send email messages directly. These blacklists can change dynamically over time, so the data doesn't need downloading or synchronising.

VPOP3 can check these RBLs for [incoming SMTP messages](#). You should only use it if the incoming SMTP is directly to your VPOP3 server. If the messages are coming through a third-party service (eg a queuing service or filtering service) before reaching VPOP3, then do *not* check RBLs. All the messages

will appear to come from the third-party service, not the sender, so checking the sender IP address will be useless and will just slow things down.

In the **RBL Servers to use** box, enter the names of the RBL services to use - eg 'zen.spamhaus.org' or 'dnsbl-2.uceprotect.net', etc.

VPOP3 will look up the IP address of the incoming sender in all the specified lists to determine if the sender is blacklisted. The blacklist will return an IP address for the name which VPOP3 looks up. By default, VPOP3 will treat the IP address as blacklisted if the blacklist returns any IP address at all (as opposed to 'name not known')

So, if you have zen.spamhaus.org, and there's an incoming connection from IP address 1.2.3.4, VPOP3 will do an A record DNS query for `4.3.2.1.zen.spamhaus.org`. If that DNS lookup returns a value, then VPOP3 will treat the sender as blacklisted.

From VPOP3 v6.17 onwards you can also specify a [regular expression](#) which must match the returned IP address for the sender to be blacklisted. To do this, specify the regular expression in parentheses immediately after the RBL name (without any spaces). For example, in the screenshot above, VPOP3 will do a DNS query to zen.spamhaus.org, and if the returning IP address matches the regular expression `127.0.0.3` then the sender will be treated as blacklisted. If any other result (or no result) is returned, then it won't be treated as blacklisted. This can be useful for some RBLs (such as zen.spamhaus.org) which return different values depending on the IP address status.

Below the RBL Servers to use box, are various options to indicate what VPOP3 should do with messages from blacklisted senders:

- **Blackhole blacklisted mail** - the message will be accepted by VPOP3 and then simply discarded. The sender will think the message was delivered, but it will not be. We do not recommend this option because it can cause confusion if a sender is on an RBL and doesn't realise it. Instead, if you do not want to receive the message, use the Reject blacklisted mail option instead.
- **Accept blacklisted mail** - VPOP3 will accept the messages and deliver them as normal. However, it will add a header beginning with the text **X-RBLFound**, such as

```
X-RBLFound: Sender address A.B.C.D found in RBL entry on YYYY
```
- **Reject blacklisted mail** - VPOP3 will do an SMTP reject on the message. The sending mail server should send a delivery failure report to the message sender. The SMTP rejection message from VPOP3 says:

```
550 5.7.1 Mail not allowed because client address A.B.C.D found in RBL entry on YYYY
```
- **Redirect blacklisted mail to ...** - VPOP3 will accept the messages, but will deliver them to the specified user, instead of the original recipient.

If the **Don't check IP addresses listed in the SMTP server access restrictions as "NOAUTH" for RBL entries** option is checked, then VPOP3 will look at the service's [IP Access Restrictions](#) and if the sender IP address is listed as "Allow Unauth" or "Allow Unauthenticated Access", then VPOP3 will skip the RBL checking.

The **IP address whitelist** lets you specify IP addresses (using [wildcards](#) if desired) which will make VPOP3 not perform RBL checking, eg `192.168.*` will make VPOP3 not perform RBL checking for any IP address beginning with "192.168."

Note that the SMTPSVR Lua script lets a script modify the RBL checking behaviour and see the results using the "Start()" and "RBLResults()" functions.

5.5.3.5.2 SPF Whitelist

To get to this page, to to [Services](#) → [SMTP Server](#) → [Spam Reduction](#) and press the **SPF Whitelist** button.

Server	IP Address	Sender Name	Sender Domain
All Servers	127.0.0.1	*	*

All Servers ▾ * *

Add Delete Close Help

SPF

SPF (Sender Policy Framework) is a way of publishing in your domain's DNS records which IP addresses are allowed to send mail from your domain. This can be used to help the recipient know that the message really came from the sender it claims to have been sent from.

Unfortunately, it is not uncommon for domain owners to publish incorrect SPF records due to not understanding them fully and not obtaining competent help. Because of this, you may need to set up 'whitelist' entries so that VPOP3 will skip SPF checks from certain sending domains or servers.

The **SPF Whitelist** screen lets you configure these whitelist entries.

To add an entry, enter the details in the four boxes above the **Add/Delete/Close** buttons, and press the **Add** button.

To delete an entry, select it, and press the **Delete** button.

To edit an entry, double-click on the cell in the table, and edit it. Changes take effect immediately.

The four options for each entry are:

- **Server** - this can be **All Servers** or **This Server**. If you have [multiple SMTP services](#) (in VPOP3 Enterprise) then this will indicate whether this SPF whitelist entry just applies to this particular service or to all of the VPOP3 SMTP services.
- **IP Address** - this indicates the sender's IP address or can be blank to indicate any sender IP address. You can use [CIDR syntax](#) in this field (eg **192.168.10.0/24**).
- **Sender Name** - this indicates the part of the email address before the @ symbol. You can leave this blank or use * to indicate any sender name. * and ? [wildcards](#) can be used in any case.
- **Sender Domain** - this indicates the part of the email address after the @ symbol. You can leave this blank or use * to indicate any sender domain. * and ? [wildcards](#) can be used in any case.

5.5.3.6 VRFY/EXPN

To get to this page, go to [Services](#) → [SMTP Server](#) → VRFY/EXPN

The screenshot shows the 'SMTP Service Configure' page for a VPOP3 server. The 'VRFY/EXPN' tab is selected. The page title is 'SMTP Service Configure' and it has a 'Submit' button. The 'VRFY and EXPN support' section is visible, with the following text: 'VRFY and EXPN are SMTP commands which allow a computer to verify email addresses without sending mail to them. Usually this is disabled for security reasons, but you may have some other software which requires their use, in which case you can enable them, but you should restrict access to only those computers which you trust.' There is a checked checkbox for 'Enable VRFY and EXPN SMTP commands (usually disabled for security reasons)'. Below this is the 'VRFY/EXPN access restrictions' section, which defines the network address & subnet masks for the computers which are allowed to use the VRFY and EXPN commands if they are enabled. There is an unchecked checkbox for 'Use Global Access Restrictions if more restrictive'. A table lists the current access restrictions:

Restrict	Type	Address	Prefix
Allow	IPv4	64.142.100.176	/28
Allow	IPv4	65.119.39.192	/27
Allow	IPv4	192.168.57.0	/24
Allow	Local Nets		

Below the table are 'Add' and 'Remove' buttons. At the bottom, there is a 'Detected Network Info' section showing: 'Routers: 192.168.66.1' and 'Networks: 127.0.0.0/8, 192.168.66.0/24, FE80::/64, ::1/128'. A note at the bottom states: '(Note that the default settings might not be correct, especially if the VPOP3 server has a direct connection to the Internet. Check the settings before accepting them!)'

The SMTP commands VRFY and EXPN are commands which allow a client to verify (VRFY) and expand (EXPN) email addresses to check that they exist, and find out what they resolve to (eg for distribution groups & aliases). For security reasons they should usually be disabled, and the default configuration in VPOP3 is that they are disabled. However, in some situations they may be useful, for instance, third party software may use these commands to check that email addresses are valid. We recommend that you only enable these commands if you know they are going to be used legitimately, and that you restrict access to the commands as much as possible.

To enable the commands, check the box **Enable VRFY and EXPN SMTP commands**.

To restrict which IP addresses can use the commands, use the [access restrictions](#) section on this page to indicate which computers can use the VRFY and EXPN commands.

5.5.3.7 Advanced

To get to this page, to to [Services](#) → [SMTP Server](#) → Advanced

The screenshot shows the 'SMTP Service Configure' page in the VPOP3 administration interface, specifically the 'Advanced' tab. The page is titled 'SMTP Service Configure' and has a 'Submit' button in the top right corner. The left sidebar shows a tree view of services, with 'SMTP Server' selected. The main content area is divided into several sections:

- Host name:** A text input field containing 'lmail.pscs.co.uk' with a note '(leave blank to use default setting)'.
- Refuse SMTP Connections from:** A text input field, currently blank, with a note '(normally left blank)'. Below it are several checkboxes:
 - Disable DSN (Delivery Status Notification) support** (this should usually be turned off (DSN Enabled))
 - Don't allow addresses with '%' in their address** (recommended, usually enabled)
 - Don't allow addresses with '!' in their address** (recommended, usually enabled)
 - Add Date: header field to locally sent messages if it doesn't exist**
 - Add original recipients to custom header if message delivered to local mailbox**
 - Log Rejected unrecognised recipients** (with a 'View Log' button)
- Maximum line length:** A text input field containing '0' with a note '(usually 0 for no limit, or 998 to be strictly RFC 5321 compliant)'.
- Max failed login attempts:** A spinner control set to '3' with a note 'per session (then connection drops)'.
- Block outgoing messages if over:** Two spinner controls, both set to '0', with a note 'messages in the Outqueue (0=no limit)'.
- Minger:** A section with a description: 'Minger is a draft protocol for verifying email addresses quickly. It is most commonly used by security edge servers or backup mail servers for verifying addresses on this server. If you have another server 'LAN Forwarding' messages to VPOP3, then using 'Minger' rather than Call-forward verification (if possible) will speed up recipient checking.' Below the description is a checkbox:
 - Enable Minger server on UDP port 4069**
- Minger Secret:** A text input field containing 'JD_%BM7O31*RRJUL' with a note '(Shared secret with Minger client)'.
- Remember recipients for Webmail:** A section with a description: 'VPOP3 can add recipients to a user's "collected addresses" when they send a message using SMTP. This can help by auto-completing that address when they subsequently send a message using Webmail. However, it does add unnecessary load to the server if most or all users usually use SMTP for sending messages.' Below the description are two checkboxes:
 - SMTP server should collect email addresses for authenticated users**
 - Only collect email addresses for users who have Webmail permission**
- Only collect addresses if user has logged into Webmail within last:** A spinner control set to '365' with a note 'days (0 = disable check)'.

The bottom of the page shows the status bar: 'VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 | idle | In: 51380 | Out: 1'.

The SMTP Advanced tab has lots of extra settings on.

Host Name sets the name which this VPOP3 SMTP service displays in its welcome banner. If this is left blank, then VPOP3 uses the **VPOP3 Host Name** setting from the [Misc Settings](#) tab.

The **Refuse SMTP Connections from** setting is rarely needed and should usually be left blank but is here for historical purposes. If you put some text in this box, then VPOP3 will refuse SMTP connections from senders whose HELO/EHLO command contains the text specified here. Eg, if this is set to *.myisp.com*, then VPOP3 will refuse SMTP connections if the sender sends a command like *HELO svr23.myisp.com*.

The **Disable DSN support** option disables the SMTP DSN (Delivery Status Notifications) extension ([RFC 3461](#)) - note not 'DNS' (Domain Name Service). This extension specifies a more structured & manageable way of sending delivery status notifications to the message sender. Usually DSN support should be enabled (so this box should be left unchecked).

The **Don't allow addresses with '%' in their address** option prevents senders sending messages to recipients containing % characters in their email address.

According to the standards, the '%' character is allowed in the 'local part' of email addresses (the part before the @ symbol). However, it is rarely used in practice.

In the 'old' days, using the percent symbol in an email address had a common use (known as the ['percent hack'](#)) which quickly became abused when spam started being created. You used to be able to send a message to something like 'bill%microsoft.com@apple.com', and the message would be sent to Apple's mail servers who would strip the @apple.com, and replace the last % with a '@' symbol, and forward the message on. This could be used legitimately for reaching mail servers which may not have very good Internet connectivity, as you could specify a route.

Note that VPOP3 will not interpret the % symbol this way, but spammers will still try to use this trick, so, unless you specifically want to allow % characters in email addresses, turning it off will submit VPOP3 to less load from spammers trying it on. Also, some security scanning software may throw an alert if it sees that VPOP3 accepts the % symbol, even though it's actually perfectly safe.

The **Don't allow addresses with '!' in their address** option prevents senders sending messages to recipients containing ! characters in their email address.

According to the standards, the '!' character is allowed in the 'local part' of email addresses (the part before the @ symbol). However, it is rarely used in practice.

Some Linux servers used to use the '!' ('bang' character) as an indication to run a command with the received email. So, sending a message to '!bin/bash+rm+-rf+/@yourcompany.com' might make your mail server delete itself...

For obvious reasons this is not widely implemented today, and VPOP3 certainly doesn't interpret the ! symbol this way, but hackers can still try to use it, so turning off VPOP3's support for ! symbols in email addresses just makes VPOP3 look safer.

The **Add Date: header field to locally sent messages if it doesn't exist** option tells VPOP3 to add a 'Date:' header field to locally sent messages if it doesn't already exist.

The Date: header field is one of the few mandatory header fields, so all email sending software should automatically add it, but occasionally you may encounter some bespoke email software which doesn't add the header correctly, so you can turn this option on to make VPOP3 add one in that case. If all sending software is correctly implemented, then this option will do nothing.

The **Add original recipients to custom header if message delivered to local mailbox** option tells VPOP3 to add custom headers listing recipients if a message is delivered to a local mailbox.

When a message is received using SMTP, then the recipients are specified using an SMTP Envelope which contains the addresses of the sender and recipients. When a mail server, such as VPOP3, delivers the message into a user's mailbox the envelope is discarded as it is of no further use.

In some cases, the mailbox may be accessed by some other software (such as another instance of VPOP3) for delivery to another site with further sorting based on message headers. In this case, BCCd messages can be misdelivered, because the envelope information has been discarded, and the message headers do not contain details of the BCC recipients.

Turning this option on will make VPOP3 add the SMTP envelope data as new lines in the message headers beginning with X-VPOP3-ORIGRCPT. These can then be used by the onward mail sorting software to see who the message recipients were. The downside is that there may be privacy implications as BCCd recipients are now listed in the message headers.

The **Log Rejected unrecognised recipients** option tells VPOP3 to log unrecognised incoming recipients into a log file.

The VPOP3 SMTP service will usually reject unknown local recipients with an error message back to the sender. In most cases this is sufficient as it means that the sender is notified, and the message will not generate error messages later.

However, in some cases, administrators may be interested in this, so you can turn this option on to make VPOP3 log the failed recipients into a *badsmtprecipients.log* log file, and you can use the *View Log* button to view the log file.

The **Maximum line length** option lets you tell VPOP3 the maximum length of a line to allow using SMTP. The SMTP standard says that incoming lines should be no longer than 1000 characters including the trailing CR/LF character pair. So, if you set this option to 998 (1000-2) then VPOP3 will be strictly SMTP compliant. If you leave it at the default 0, then VPOP3 will not limit line lengths at all. VPOP3 is totally safe to have longer line lengths than 1000 characters, but some security testing software will mistakenly assume that if the server doesn't check the line length then there is the risk of a 'buffer overflow vulnerability'. This is incorrect in the case of VPOP3, but this setting allows you to tell VPOP3 to restrict line lengths so that the security testing software will be satisfied.

The **Maximum failed login attempts** option lets you specify how many failed attempts to log in are allowed before VPOP3 will drop the connection so the sender will have to reconnect to try again. This allows persistent attackers to be rejected and blocked by VPOP3. The [security checking](#) part of VPOP3 only checks for this at the start of a connection, so if this is set too high then an attacker will be able to make many attempts before being blocked.

The **Block outgoing messages if over X messages in the Outqueue** option tells VPOP3 that if this many messages are waiting to be sent out from VPOP3, it will prevent users from sending any more messages. This lets you set protection against outgoing spam attacks due to misconfiguration or discovered passwords. If you set this to a number higher than you would normally expect to see in the VPOP3 Outqueue then it will allow normal sending operation, but the damage from any outgoing spam attack will be reduced because VPOP3 will prevent many thousands of outgoing messages from being sent.

The **Block outgoing messages if over X messages in the Outqueue from this user** option is the same as above, but only checks messages from the same authenticated user. This option will not check unauthenticated outgoing messages.

Minger

Minger (**M**ail **p**INGER) is a [draft Internet protocol](#) used between mail servers to allow authenticated verification of email addresses. This can be useful if one server is forwarding mail onto another server; it can use Minger to check the recipient email address is valid automatically without having to have a complete list of valid addresses maintained on the second server.

As this protocol is authenticated, it can be left safely running, and it will not leak information, or cause any noticeable server load, even if it is not in use. However, you can turn it off if you wish if it is not being used.

The **Minger Secret** is a 'password' which is shared between the Minger client and the Minger Server.

VPOP3's [LAN Forwarding Configuration](#) supports the use of Minger when LAN forwarding wildcarded email addresses to another server.

Remember recipients for Webmail

VPOP3 will autocomplete recipients when messages are being sent from Webmail. Usually it will only remember (and thus autocomplete) recipients sent to from within Webmail.

If **SMTP server should collect email addresses for authenticated users** is checked, then VPOP3 will also remember recipient email addresses when users send from a normal email client as well as from Webmail.

The **Only collect email addresses for users who have Webmail permission** option tells VPOP3 to only remember email addresses if the user has [permission to use Webmail](#). This isn't vital, but it can help to reduce the space needed for VPOP3 to store the remembered addresses that will never be used.

The **Only collect addresses if user has logged into Webmail within last X days** option tells VPOP3 to only remember email addresses if the user has used Webmail within the specified number of days. This isn't vital, but it can help to reduce the space needed for VPOP3 to store the remembered addresses that are unlikely to be used.

5.5.3.8 IDS/IPS

To get to this page, to to [Services](#) → [SMTP Server](#) → IDS/IPS

The screenshot shows the 'SMTP Service Configure' interface with the 'IDS/IPS' tab selected. The 'Intrusion Detection/Prevention' section is active, with the following settings:

- Enable IDS Logging:** (disabled)
- IDS Log Filename:** ids.log
- IDS Log Line Format:** %T - %I - %e %E - %D
- Intrusion Prevention Multipliers:**
 - Client Error Monitor Period: 60 minutes
 - Client Error Block Time: 30 minutes
 - Bad Authentication Multiplier: 50
 - Relay Allowed Multiplier: 1
 - Good Local Rcpt Multiplier: 0
 - Virus Detected Multiplier: 200
 - DNSBL Match Multiplier: 200
 - Message Too Big Multiplier: 10
 - Partial Attachment Multiplier: 100
 - Client Error Block Threshold: 1000
 - Client Error Re-Block value: 800
 - Relay Denied Multiplier: 100
 - Bad Local Rcpt Multiplier: 50
 - Spam Detected Multiplier: 50
 - SMTP Rule Reject Multiplier: 200
 - Syntax Error Multiplier: 50
 - Filtered Attachment Multiplier: 50

Buttons at the bottom include 'Manage Block List', 'Manage Never Block List', and 'View Event Log'. The status bar at the bottom shows 'VPOP3 Enterprise 6.20 - pscs2.co.uk - FD00:F0F2:498F:5FF2:2480:EC9C:A597:6EAD | Idle | In: 89 | Out: 12'.

The IDS (Intrusion Detection System) & IPS (Intrusion Prevention System) options in VPOP3 let VPOP3 detect and prevent 'bad' computers from connecting to it.

Intrusion Detection

The IDS component is most useful if linked with some other software which can parse the logs and either generate useful reports or update firewall rules dynamically.

The IDS component will optionally log 'suspicious' behaviour to a specified file (**IDS Log Filename**). Third party software can monitor this log file and do what you want it to do. Note that VPOP3 will not

manage the size of this log file in any way, so you should have some other means of controlling its size. Often the IDS log parser software can empty/rotate the log file for you or there are programs like [LogRotateWin](#) which you can configure to do that for you.

The **IDS Log Line Format** tells VPOP3 how to format the data lines it writes to the IDS Log File. You can configure this to match a format supported by your log file parsing software. You can use replacements to indicate variable text.

- **%T** = UTC timestamp in ISO8601 format
- **%I** = the SMTP client's IP address (as seen by VPOP3)
- **%e** = the IDS event number
- **%E** = the IDS event text description
- **%D** = extra event data

You can use an [Lua script](#) to customise the line format further - eg if the timestamp needs to be in a different format

The IDS event numbers used by VPOP3 are:

0. SMTP authentication failure
1. Relay denied
2. Relay allowed (not bad in itself, but a large number may indicate an open relay or spambot, etc)
3. Bad local recipient
4. Good local recipient (not bad in itself, but a large number may indicate a spammer)
5. Message detected as spam
6. Message detected as containing a virus
7. SMTP Rule matched
8. Realtime DNS Blacklist match
9. SMTP Syntax error (commonly spam software is badly written, so these can happen if error handling is poor in the sending software)
10. Message is bigger than the maximum size limit specified in VPOP3
11. Message contained a filtered attachment
12. Message contained a partial attachment (these are often an indication of something trying to bypass virus scanners)
13. SPF Rejection
900. IP address blocked

Intrusion Prevention

The Intrusion Prevention component uses the Intrusion Detection data to automatically block IP addresses if VPOP3 detects suspicious activity from them. If this happens, the connecting computer will receive an error such as **Server access temporarily blocked! Please try again later** or **Your connection has been blocked temporarily - try again later.**

The **Manage Block List** button allows you to view blocked IP addresses and manually add or delete them. The **Manage Never Block List** button lets you add or delete IP addresses from a list of IP addresses to never block (eg trusted IP addresses).

When an incoming connection is initiated, the order of events is:

1. VPOP3 looks at the client IP address.
2. VPOP3 checks the **Never Block List**. If the IP address is there, the connection is allowed.
3. VPOP3 checks in the **Block List**. If the IP address is there, then the connection is blocked.
4. If the IP address was in the **Block List**, but the entry expired within the past **Client Error Monitor Period** time, then the IPS log total value is seeded with the **Client Error Re-Block** value. This means that a badly behaved client is more likely to be blocked again if it continues to misbehave.
5. VPOP3 checks the previous entries in the IPS event log over the past **Client Error Monitor Period** time. If the total of the entry values equals or exceeds the **Client Error Block Threshold** then the connection is added to the **Block List** with an expiry set to the **Client Error Block Time** in the future, and the connection is blocked.

If the connection is allowed, then VPOP3 will add entries to the IPS event log as they occur. These will not cause the connection to be added to the **Block List** immediately, but will only be checked at the next connection from the same IP address. This reduces computational load on the server, and means that isolated events from an IP address will not cause an entry to be added to the **Block List** which will then expire before it is used.

The various events which are logged are shown on the page as various 'multipliers'. Every time an event occurs within the Client Error Monitor Period, then the value of that 'multiplier' is added onto that IP address's "score".

Notes:

- Changing an event's "multiplier" will take effect retrospectively.
- The **Client Error Monitor Period** should not be set for longer than 30 days, as events are purged from VPOP3's internal log after 30 days
- You cannot turn off the IDS component of VPOP3. You can achieve the same effect by setting all the 'multipliers' to zero, or decreasing the Monitor Period to 1 minute and increasing the Block Threshold to an unreachable value.

Manage Block List

When a connection attempts to connect and has already logged events over the **Block Threshold**, then it will be added to the **Block List**. Addresses can also be added to the **Block List** manually.

Note that the **Block List** affects ALL VPOP3 services. It is also updated by the [Security Settings](#) in VPOP3, if someone repeatedly attempts to log in with bad details.

The **Block List** can be viewed to see which IP addresses are already in the block list, when they were added, and when they will expire. If you double-click on an entry, VPOP3 will show you why that address was added to the block list. You can delete entries from the block list.

You can manually add entries to the block list by entering the address and period that the address should be blocked, and pressing the **Add** button. The maximum time you can block an address for is

999,999,999 minutes (approximately 1900 years). The Address you specify can be an individual address, or a network range specified in [CIDR format](#) (eg 1.2.3.0/24)

Manage Never Block List

The **Never Block List** is used to tell VPOP3 never to block connections from the specified addresses. This can be useful for internal IP address ranges, or the IP addresses of partners or mail forwarding services.

Note that the **Never Block List** affects ALL VPOP3 services, and will also prevent the Security Settings options from blocking IP addresses.

The **Never Block List** can be viewed to see which IP addresses are already in the list and when they were added. You can delete entries from the block list by selecting them and pressing the **Delete** button.

You can manually add entries to the **Never Block List** by entering the address and pressing the **Add** button. If you add an entry to the **Never Block List**, then it will automatically be removed from the **Block List** if the address is currently blocked.

The Address you specify can be an individual address, or a network range specified in [CIDR format](#) (eg 192.168.0.0/16)

View Event Log

This lets you see the recent past events added to the IDS event log. Events are displayed here even if they have a zero 'multiplier' so will not prevent access to VPOP3.

5.5.4 IMAP4

The VPOP3 IMAP4 service is only available in [VPOP3 Enterprise](#) and provides [IMAP4](#) services to email clients.

➤ [General Tab](#)

➤ [IP Access Restrictions Tab](#)

➤ [Advanced Tab](#)

5.5.4.1 General

To get to this page, to to [Services](#) → [IMAP4 Server](#) → General (VPOP3 Enterprise Only)

The screenshot shows the 'IMAP4 Service Configure' interface. The left sidebar contains a tree view with 'IMAP4 Server' highlighted. The main panel has three tabs: 'General', 'IP Access Restrictions', and 'Advanced'. The 'General Settings' section is active and contains the following configuration options:

- Enable Service**
- Bindings :**

Address	Port
[Any IPv4]	143
- (default port: 143)
- Encryption :** None/STARTTLS
- Require encrypted authentication.** (This is not supported by all email clients, but means that passwords must be sent to the VPOP3 IMAP4 service in an encrypted form rather than as plain text.)
- Bandwidth Throttling:** No Limit bytes/second.
- Log data for this service**

At the bottom of the page, the status bar shows: VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 | Idle | In: 49091 | Out: 0

Service Name is a name you have given to this IMAP4 server. The name doesn't matter. It is used in the settings (in the service tree at the left of this page) and in any error messages.

The **Bindings** section is described in the [Service Bindings](#) topic.

The **Encryption** option lets you specify how connections to this IMAP4 service are encrypted. This is only available when an [SSL certificate is installed](#); it can be **None/STARTTLS**, **STARTTLS** or **SSL**. IMAP4 supports two types of encryption, STARTTLS and SSL.

STARTTLS is the standard method. With this method, connections are usually made on the standard port (143). The server indicates to the IMAP4 client that encryption is available, and the client sends a **STARTTLS** command to switch the session from plain text to the encrypted mode. No sensitive data (authentication details, message details, etc) is transmitted while the session is in plain text mode. **None/STARTTLS** means that VPOP3 offers encryption to the client, but will allow unencrypted connections. **STARTTLS** means that VPOP3 offers encryption to the client, and requires it to be used.

SSL is a deprecated method. With this method, the connection is made on a port other than port 143 (usually port 993) and starts off encrypted. This means that the IMAP4 client must know that the session is encrypted before it connects, otherwise it won't be able to establish a connection successfully.

Bandwidth Throttling allows you to set limits on how fast data will be transferred through this SMTP service. This allows you to prevent it taking up all your available bandwidth. See the [Bandwidth Throttling](#) topic for more information.

The **Log data for this service** option tells VPOP3 to log session data to a log file **IMAP4SVR.LOG** (see the [Diagnostics settings](#) for more information). It is equivalent to turning on 'Log IMAP4 Server Connections' on that page).

5.5.4.2 IP Access Restrictions

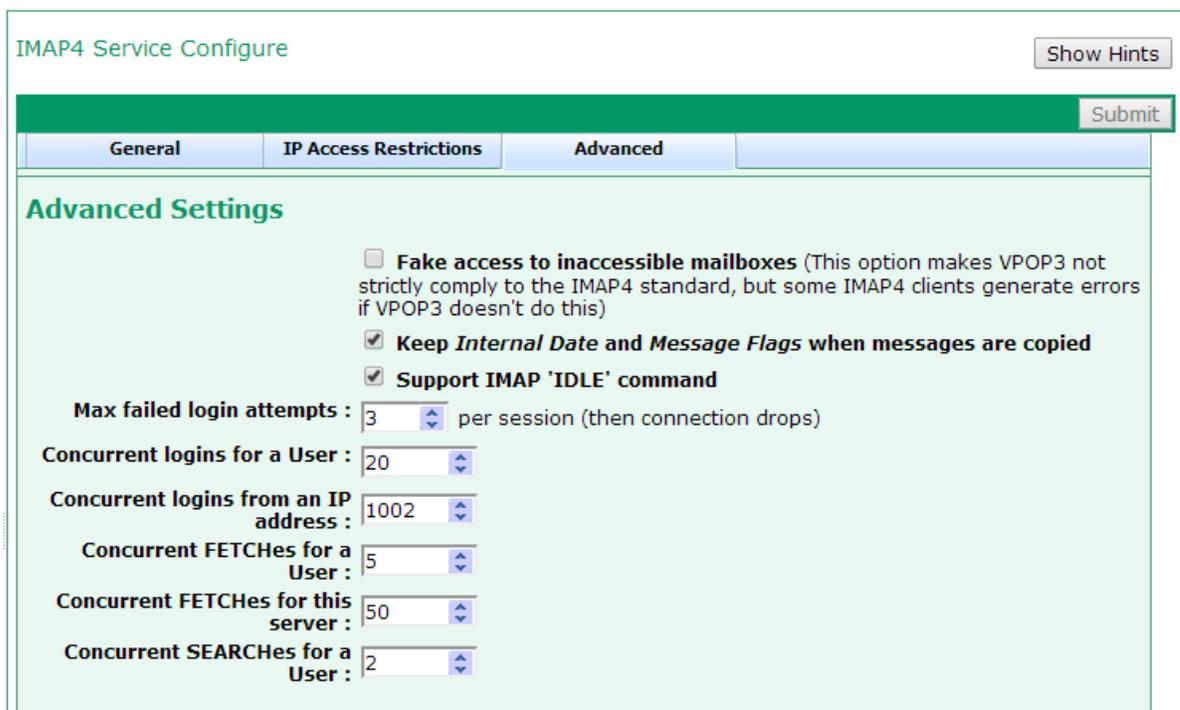
To get to this page, to to [Services](#) → [IMAP4 Server](#) → IP Access Restrictions

This tab is present for all VPOP3's Services. For general details on how this tab works, see the [IP Access Restrictions](#) section.

If the email client receives the error ***BYE VPOP3 IMAP4rev1 Server access not allowed!** then this means that the IP access restrictions are blocking access from this IP address.

5.5.4.3 Advanced

To get to this page, to to [Services](#) → [IMAP4 Server](#) → Advanced



The screenshot shows the 'IMAP4 Service Configure' interface with the 'Advanced' tab selected. The 'Advanced Settings' section includes the following options and values:

- Fake access to inaccessible mailboxes (This option makes VPOP3 not strictly comply to the IMAP4 standard, but some IMAP4 clients generate errors if VPOP3 doesn't do this)
- Keep Internal Date and Message Flags when messages are copied
- Support IMAP 'IDLE' command
- Max failed login attempts : 3 per session (then connection drops)
- Concurrent logins for a User : 20
- Concurrent logins from an IP address : 1002
- Concurrent FETCHes for a User : 5
- Concurrent FETCHes for this server : 50
- Concurrent SEARCHes for a User : 2

The IMAP4 Advanced tab lets you configure rarely used settings for the [IMAP4](#) server component of [VPOP3 Enterprise](#).

The **Fake access to inaccessible mailboxes** setting lets VPOP3 act in a way which enables older IMAP4 email clients to work better. In the IMAP4 service you may have folders which do not exist. For instance, if you are accessing a shared Inbox folder from a user called 'Karen', then their folder will be called `#users/Karen/Inbox`. The `#users` and `#users/Karen` folders are not actually present, but will be displayed in a folder tree. This can upset some older email clients, so VPOP3 can pretend those folders exist, but don't contain any messages.

For strict IMAP4 standard compliance the **Keep Internal Date and Message Flags when messages are copied** option should always be checked, but in some cases people have preferred for it not to be checked. Each message has meta-data containing the Internal Date (when VPOP3 received the message) and Message Flags (read, deleted, flagged, replied etc). If this option is unchecked, then when messages are copied to another folder, this meta-data is reset.

The **Support IMAP 'IDLE' command** option lets you enable or disable VPOP3's support for the **IDLE** command. The [IMAP IDLE](#) command is a way of implementing 'push' notifications to an IMAP4 client. Normally, you would want this option to be turned on, but in some cases it has caused reliability issues, so it can be turned off if necessary.

The **Max failed login attempts** option tells VPOP3 how many failed login attempts to allow before dropping the connection. The default is 3.

The **Concurrent logins for a user** option limits the number of concurrent logins for a particular user. The main purpose for this option is that some email clients will connect to an account and instantly open up a connection for each mail folder which exists in that account. In some cases this can mean that VPOP3 suddenly has to handle 200+ new connections. It will do this, but it may take some time - the problem is that some clients will time out while this is happening, and will reconnect with a new 200+ connections. After a short time VPOP3 will grind to a halt processing new logins for a single user. Most well-behaved clients will limit themselves to 3-5 connections, so allowing 20 concurrent connections will allow about 4 people/devices to access the same mailbox at once. If you know that your clients are well-behaved you can increase this as necessary. If the limit is reached, then further attempts to log in will receive an error message *Too many logins for this user*.

The **Concurrent logins from an IP address** setting is similar to the above setting, but restricts the number of logins from a single IP address. This is usually set much higher than the previous setting, because people often connect to VPOP3 over a shared connection, so many users will have the same IP address. If the limit is reached, then further attempts to log in will receive the error message *Too many connections from this address!*

The **Concurrent FETCHes for a user** option lets you limit how many concurrent message FETCH commands VPOP3 will run for a specific user. Usually there will just be one or two FETCHes running at once, but badly behaved clients have been known to issue lots of FETCH commands which can overload the server. If more FETCH commands are issued than this option allows, VPOP3 will queue them up and wait for up to 40 seconds for a current FETCH command to finish. If no free FETCH 'slots' are available then an error *Too many current FETCHes active* will be returned.

The **Concurrent FETCHes for this server** option lets you limit how many concurrent message FETCH commands VPOP3 will run on the whole server. If there are too many concurrent FETCH commands it can overload the server. If more FETCH commands are issued than this option allows, VPOP3 will queue them up and wait for up to 40 seconds for a current FETCH command to finish. If the timeout is reached then an error *Too many current FETCHes active* will be returned.

The **Concurrent SEARCHes for a user** option lets you limit how many concurrent message SEARCH commands VPOP3 will run for a specific user. Usually there will just be at most one SEARCH running at once. SEARCH commands can be very time consuming and put load on the server, especially with large mail folders, so it is best to keep this to a small limit to avoid overloading the server. If more SEARCH commands are issued than this option allows, VPOP3 will queue them up and wait for up to 30 seconds for a current SEARCH command to finish. If the timeout is reached then an error *Too many concurrent searches - try again later* will be returned.

With the various **Concurrent** limits, the main risk is that email clients will sometimes retry actions if the previous attempt took too long. This will mean that if the client retries after 60 seconds, and a SEARCH, for instance, will take 5 minutes, then the email client will issue a duplicate SEARCH command after 1 minute. VPOP3 will now be doing the SEARCH twice, which will take even longer. Then after another minute, the email client will issue another duplicate SEARCH command, slowing things down further. After a few minutes the server will have ground to a halt trying to process many identical SEARCH commands. There is not really a nice way around this from the server's point of view other than to block extra commands which is what these options allow. The email client should not really retry commands

unless it has received an error such as the connection being dropped, or it should wait a lot longer than 1 minute.

5.5.5 Password

The VPOP3 Password service allows some email clients to change the account password remotely

➤ [General Tab](#)

➤ [IP Access Restrictions Tab](#)

Note that this service is disabled by default on new installations of VPOP3 because there are no known current email clients which support this system. It used to be used by the Eudora email client, but that email client is now no longer published.

5.5.5.1 General

To get to this page, to to [Services](#) → [Password Server](#) → General

The **Enable Service** box lets you enable or disable the service. This service is usually disabled because it is not used by any known current email clients.

The **Bindings** section is described in the [Service Bindings](#) topic.

Bandwidth Throttling allows you to set limits on how fast data will be transferred through this SMTP service. This allows you to prevent it taking up all your available bandwidth. See the [Bandwidth Throttling](#) topic for more information.

5.5.5.2 IP Access Restrictions

To get to this page, to to [Services](#) → [Password Server](#) → IP Access Restrictions

This tab is present for all VPOP3's Services. For general details on how this tab works, see the [IP Access Restrictions](#) section.

5.5.6 Finger

The VPOP3 Finger service allows supports the [Name/Finger protocol](#)

➤ [General Tab](#)

➤ [IP Access Restrictions Tab](#)

Note that this service is disabled by default on new installations of VPOP3 because it is generally considered insecure and unsafe. In some situations it may be a reasonable service to provide, but you should use the IP Access Restrictions to prevent access to the Finger service from outside your network.

5.5.6.1 General Tab

To get to this page, to to [Services](#) → [Finger Server](#) → General

The **Enable Service** box lets you enable or disable the service. This service is usually disabled because it is generally considered insecure.

The **Bindings** section is described in the [Service Bindings](#) topic.

Bandwidth Throttling allows you to set limits on how fast data will be transferred through this SMTP service. This allows you to prevent it taking up all your available bandwidth. See the [Bandwidth Throttling](#) topic for more information.

The Finger protocol returns text - in either a verbose or normal response. The administrator can define a template which defines the text returned. The template can contain plain text, with some tags (defined as displayed below the template box - eg **<id>** for the account name).

The *Plan* and *Info* text is defined in the [Edit User](#) window for the user, in the **Finger Info** tab.

5.5.6.2 IP Access Restrictions

To get to this page, to to [Services](#) → [Finger Server](#) → IP Access Restrictions

This tab is present for all VPOP3's Services. For general details on how this tab works, see the [IP Access Restrictions](#) section.

5.5.7 LDAP

The VPOP3 LDAP service allows supports the LDAP protocol to access the [global address book](#) from email client software.

- [General Tab](#)
- [IP Access Restrictions Tab](#)
- [Advanced Tab](#)

5.5.7.1 General

To get to this page, to to [Services](#) → [LDAP Server](#) → General

VPOP3 Enterprise 7.0 - lmail.pscs.co.uk - 192.168.66.23 | Idle | In: 38507 | Out: 0

The **Enable Service** box lets you enable or disable the service.

The **Bindings** section is described in the [Service Bindings](#) topic. The standard port for LDAP is port 389. If VPOP3 is running on a Windows Active Directory server, then Active Directory requires *its* LDAP server to use port 389, so VPOP3 will usually run its LDAP service on an alternative port, such as port 1389.

If the **Require Authentication** option is checked, then users need to authenticate their LDAP connections before address details can be accessed. If it is not checked, then the LDAP connection is unauthenticated and anyone who can access the VPOP3 server can access the global address book. Note that personal and shared address books (in VPOP3 Enterprise) require authentication for access.

If the **Allow Modification of Global Address Book** by users option is checked, then any user can modify the [Global Address Book](#) through their Webmail login. If it is not checked, then users can only

modify their own personal address book, or shared address books that they have write access to (in VPOP3 Enterprise only).

Bandwidth Throttling allows you to set limits on how fast data will be transferred through this SMTP service. This allows you to prevent it taking up all your available bandwidth. See the [Bandwidth Throttling](#) topic for more information.

Note that the LDAP protocol does not support the modification of entries very well, so neither email clients nor VPOP3 support that facility. To modify address book entries, users have to use Webmail (or the Administrator settings).

5.5.7.2 IP Access Restrictions

To get to this page, to to [Services](#) → [LDAP Server](#) → IP Access Restrictions

This tab is present for all VPOP3's Services. For general details on how this tab works, see the [IP Access Restrictions](#) section.

5.5.7.3 Advanced

To get to this page, to to [Services](#) → [LDAP Server](#) → Advanced

The screenshot shows the VPOP3 Enterprise 7.0 Admin Settings interface. The top navigation bar includes icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, and Help. The left sidebar shows a tree view of server configurations, with 'LDAP Server' selected. The main content area is titled 'LDAP Service Configure' and has a 'Show Hints' button. Below the title is a 'Submit' button. The 'Advanced' tab is active, showing 'Advanced Settings'. The settings include a checked checkbox for 'By default return all available attributes' and an unchecked checkbox for 'Use ODBC database as well as local database'. A 'Configure ODBC' button is located below the second checkbox. The status bar at the bottom indicates 'VPOP3 Enterprise 7.0 - Imail.pscs.co.uk - 192.168.66.23', 'Idle', 'In: 38507', and 'Out: 0'.

The LDAP Advanced tab lets you configure rarely used settings for the LDAP server component..

If the **By default return all available attributes** option is checked, then if an LDAP client doesn't specify which attributes it wishes, VPOP3 will give it all the available attributes. If this option is not checked, VPOP3 will only return a restricted set of attributes. This option should always be turned on.

With [VPOP3 Enterprise](#), you can tell VPOP3 to access an external address book database using an [ODBC driver](#). VPOP3 can then provide contact details from this external database to people using the VPOP3 LDAP or [Webmail](#) services. This is an advanced feature and requires you to install and configure a suitable ODBC driver on the VPOP3 computer and know details of the database schema you are connecting to. See the [ODBC Database](#) topic for more information.

5.5.7.3.1 ODBC Database

In [VPOP3 Enterprise](#), you can have VPOP3 retrieve address book contents from an external database using [ODBC](#) (Open DataBase Connectivity) to allow users to access addresses from a separate company database as well as the built-in [address book](#) in VPOP3.

LDAP is a hierarchical system with many different attributes and object types which doesn't map nicely onto a standard database record format. So, the ODBC->LDAP gateway in VPOP3 only supports a subset of LDAP features. In most cases users won't notice anything when using normal email client software, but if you are using software which uses certain features of LDAP, then that software may have problems with data from the ODBC database.

Configuring the ODBC Driver

To use the ODBC gateway you need to first configure a suitable ODBC driver on the VPOP3 PC. This must be a 32 bit or 64 bit ODBC driver to match the 32 or 64 bit version of VPOP3, and must be a 'System' driver (not for the current user, because VPOP3 runs as a service, not in the current user's account).

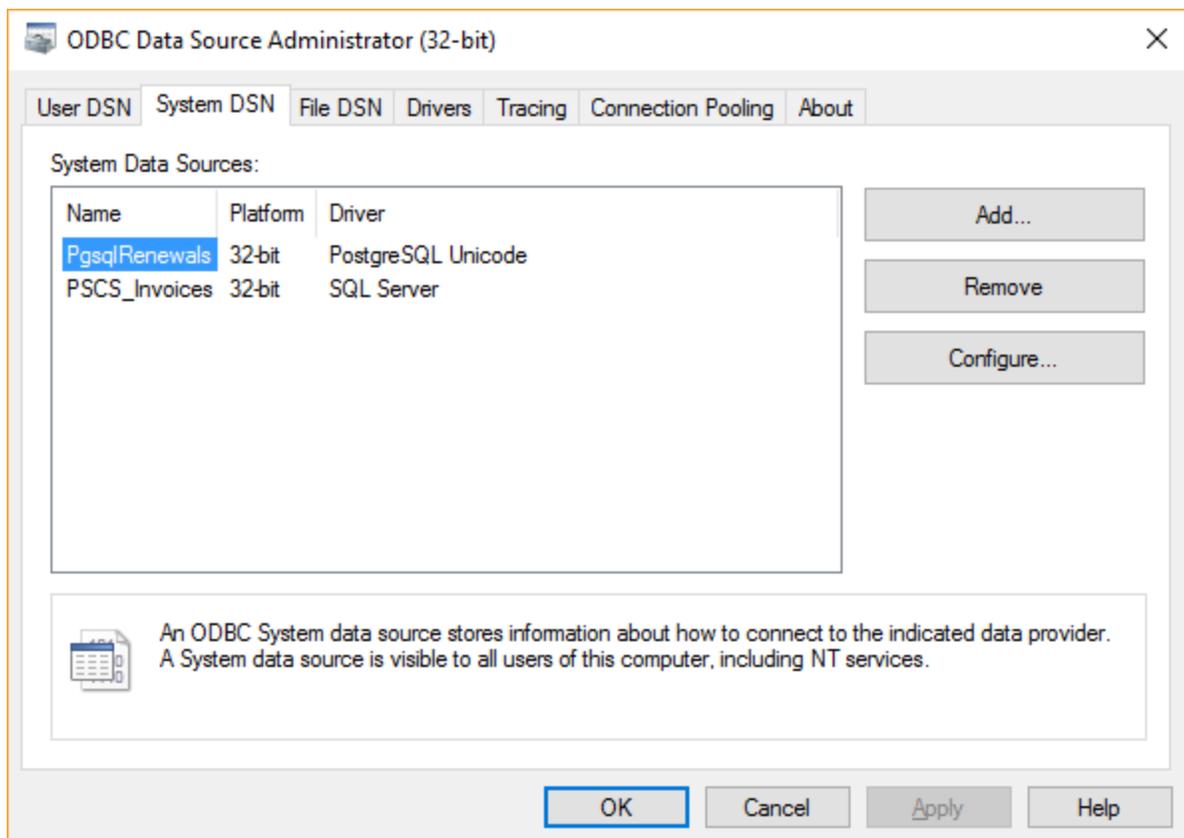
To do this, go to the appropriate directory as below and run **odbcad32.exe**

- 32 bit VPOP3 on 32 bit Windows - *c:\windows\system32*

- 32 bit VPOP3 on 64 bit Windows - *c:\windows\syswow64*

- 64 bit VPOP3 on 64 bit Windows - *c:\windows\system32* (note that the program is still odbcad32.exe and it's in the 'system32' folder even though it's a 64 bit version...)

Go to the **System DSN** tab. (DSN stands for 'Data Source Name' and is the way databases are referred to in ODBC).



Press **Add** and choose the appropriate ODBC driver, and configure it as appropriate. Unfortunately, we cannot give details here because there are many ODBC drivers and they need different settings. The documentation for the ODBC driver you are using should tell you how to configure it. If the database type you want is not shown, then you may need to install an ODBC driver for it - see the documentation for the database you want for details.

Unfortunately, this section is vague, because all this depends on which database you need, whether there's an ODBC driver for it, and how you obtain the ODBC driver and configure it can be very different for different databases

Configuring VPOP3

Once you have the ODBC driver installed on the VPOP3 PC, then you can go to [Services -> LDAP -> Advanced](#), check the **Use ODBC database as well as local database** box and press the **Configure ODBC** button. This should show all the ODBC DSNs available to VPOP3.

Configure LDAP ODBC Settings

Data Source : PgsqIRenewals
PSCS_Invoices

Username if needed :

Password if needed :

If the DSN you want is not available, then you haven't configured it correctly in the ODBC setup. Check that it is configured in the **System DSN** tab, not the **User DSN** tab. Also check that you have used the correct version of **odbcad32** - if you configure the DSN in the 64 bit version, it will not be available to the 32 bit version of VPOP3, and vice versa.

If the DSN you want is available, then select it, and enter the username & password needed to connect to the database (if any) and press **Next**. If the username & password are correct, then the next page should show you all the database tables and views available to that user.

Configure LDAP ODBC Settings

Data Source :

Data Table :

"WHERE" clause (optional) :

Use *SELECT DISTINCT*

LDAP Attributes

Display Name :

Email Address :

Job Title :

First Name :

Middle Initials :

Family Name :

Key column (unique index) :

Now, you can specify a WHERE clause to filter the data if you wish.

If the table may contain duplicate entries, checking the **Use SELECT DISTINCT** may help (it's better to use a custom view if possible).

You can also link some standard LDAP attributes to the relevant table columns. If the database table does not contain certain data, then just leave it set to **<None>** and the LDAP service will not return data for that attribute.

There *must* be a unique id column in the table which VPOP3 can use to identify a value. Specify that in the **Key column** setting.

Press **Finish** once you have finished, and the VPOP3 LDAP service will return the database data to any LDAP clients.

Technical note - the LDAP data is returned as children of the **OU=ODBC,OU=EXTERNAL,O=VPOP3** LDAP DN (distinguished name), so if you want the email client to only see this data, set that DN as the 'base DN' in the email client's LDAP configuration.

5.5.8 WebMail

The VPOP3 Webmail service provides Webmail, administration and CalDAV services to users & administrators.

You access the Webmail service by going to **http://<server address or name>:5108**

(The :5108 is because, by default, VPOP3 installs its Webmail service on port 5108 so as not to conflict with an existing Web server on the same computer. There is no reason not to change it to use port 80 (or 443 if you are using encryption in VPOP3 Enterprise)

The login details for both Webmail and administration are usually the same as your login details for accessing the POP3/SMTP/etc services.

- [General Tab](#)
- [IP Access Restrictions Tab](#)
- [WebMail Settings Tab](#)
- [WebAdmin Settings Tab](#)
- [Advanced Tab](#)
- [Collected Addresses Tab](#)

5.5.8.1 General

To get to this page, to to [Services](#) → [Webmail Server](#) → General

The screenshot displays the 'Web Mail Service Configuration' interface. The left sidebar shows a tree view of services, with 'WebMail Server' selected. The main content area is titled 'Web Mail Service Configuration' and has a 'Submit' button. Below this is a tabbed interface with tabs for 'General', 'IP Access Restrictions', 'WebMail Settings', 'WebAdmin Settings', 'Advanced', and 'Collected Addresses'. The 'General Settings' tab is active, showing the following configuration:

Bindings :

Address	Port
[Any]	5108
[Any IPv4]	80
[Any IPv4]	6000

Below the table is an 'Edit Bindings' button with the text '(default port: 5108 - change with caution)'.
Encryption : SSL (selected in a dropdown menu)
Logon Idle Timeout : 3 minutes (with up/down arrows)
Bandwidth Throttling : No Limit (selected in a dropdown menu) 1000000 bytes/second.

At the bottom of the interface, the status bar shows: 'VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23' and 'Idle | In: 46254 | Out: 0'.

The **Bindings** section is described in the [Service Bindings](#) topic. The Webmail service defaults to listen on port 5108. It can use port 80 or port 443 as long as there are no other web servers on the same IP address.

The **Encryption** option is only available in VPOP3 Enterprise when an [SSL certificate is installed](#); VPOP3 Basic does not support encryption here. It can be **None**, **SSL** or **Autodetect**.

SSL means that VPOP3 will always require the **https://** protocol to access it. In this case, if it detects an incoming **http://** connection, it will redirect it to the **https://** connection.

None means that VPOP3 will always require the **http://** protocol to access it.

Autodetect means that VPOP3 will look at the start of an incoming connection to try to determine whether **http://** or **https://** is being used and will adapt accordingly.

The **Logon Idle Timeout** setting indicates how long an idle session should be before VPOP3 times it out and logs it out. Note that if the web page is left open, periodic background updates will probably keep the session active, but if the web browser is closed down, these will stop meaning the session will time out.

Bandwidth Throttling allows you to set limits on how fast data will be transferred through this SMTP service. This allows you to prevent it taking up all your available bandwidth. See the [Bandwidth Throttling](#) topic for more information.

5.5.8.2 IP Access Restrictions

To get to this page, to to [Services](#) → [Webmail Server](#) → IP Access Restrictions

This tab is present for all VPOP3's Services. For general details on how this tab works, see the [IP Access Restrictions](#) section.

5.5.8.3 WebMail Settings

To get to this page, to to [Services](#) → [Webmail Server](#) → Webmail Settings

The screenshot displays the VPOP3 Web Mail Service Configuration interface. The top navigation bar includes links for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. The left sidebar shows a tree view of services, with 'WebMail Server' selected. The main content area is titled 'Web Mail Service Configuration' and features a 'Submit' button. Below this is a tabbed interface with tabs for General, IP Access Restrictions, WebMail Settings (selected), WebAdmin Settings, Advanced, and Collected Addresses. The 'WebMail Settings' tab contains the following configuration options:

- Max Messages per page: 10000
- Max Address Book Entries per page: 100
- Allow WebMail Email Address Settings by users
- Restrict Autoresponder options when set by user (Prohibit including files etc)
- Allow Rich-text editor in IE/Mozilla
- Enable Spell Checker
- Disable all links in messages
- Spell Checker Dictionaries: British English (dropdown menu)
- Edit company dictionary (button)
- Default WebMail language: english (dropdown menu)
- Login Logo: Choose file (No file chosen), Upload, Delete (width:104 pixels x height:86 pixels)
- Webmail Logo: Choose file (No file chosen), Upload, Delete (width:200 pixels x height:47 pixels)

At the bottom of the interface, the status bar shows 'VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23' and session information: 'Idle | In: 46256 | Out: 0'.

Max Messages per page indicates the maximum number of messages in a Webmail page. The user can set the number of messages in a page themselves, but this setting sets the maximum number that the user is allowed to set. The larger the number the user chooses the less paging needs to be performed by the user, but the slower loading will be.

Max Address Book Entries per page is the same as above, but for address book entries rather than messages

The **Allow Webmail Email Address Settings by users** option allows users to set their own email addresses in their Webmail settings. If this is disabled, then users' email addresses have to be set by the administrator. (This is used when the user has several email addresses they may send messages from.)

The **Restrict Autoresponder options when set by user** option restricts options that users can select for autoresponders, such as including files from disk etc. This should usually be turned on.

Allow Rich-text editor in IE/Mozilla enables a rich-text editor when composing a message in Webmail. This should usually be turned on. If it is off, then only a basic plain-text editor is supported.

The **Enable Spell Checker** option enables a spell checker in the rich-text editor when composing a message.

The **Disable all links in messages** option makes VPOP3 inactivate any links in messages. This means that users can't click on links to go to other sites. This may be seen as a security benefit, but can also be confusing and inconvenient for users.

VPOP3 comes with several **Spell Checker Dictionaries**, you can select from them using the **Spell Checker Dictionaries** drop-down box.

The **Edit company dictionary** button lets you specify a list of words to be added to a company-wide dictionary for the spell checker. Each user also has their own dictionary which they can maintain themselves.

You can specify logos to add to the Webmail login page and to the top-right of the Webmail pages using the **Login Logo** and **Webmail Logo** options. The logo sizes are displayed for your reference. If you use other sizes then they will be rescaled which may make them look odd.

5.5.8.4 WebAdmin Settings

To get to this page, to to [Services](#) → [Webmail Server](#) → Webadmin Settings

The **Settings start page** option simply indicates whether you are taken to the [Status](#) page or [Users](#) page after logging into the admin settings.

The **Admin Area Access Restrictions** are a second set of [IP Access Restrictions](#) which restrict which IP addresses/users can access the Admin settings (obviously users need to be Administrators too). Users need to first have access using the base [IP Access Restrictions](#) to be able to log into Webmail at all, and then have access through the **Admin Area Access Restrictions** to be able to access the VPOP3 Admin settings. If this list of restrictions is empty, then any administrator who can access the Webmail service can also access the Admin settings.

5.5.8.5 Advanced

To get to this page, to to [Services](#) → [WebMail Server](#) → Advanced

The screenshot shows the 'Web Mail Service Configure' interface with the 'Advanced' tab selected. The 'Advanced Settings' section includes several checked options: 'Allow Password in URL', 'Allow different client addresses for a Web Mail session', 'Support CalDAV scheduling extension', and 'Support different CalDAV authentication realms for different accounts'. A text field for 'Mail HTML Pages' contains 'c:\vpop3_webmail'. Below this are three unchecked options: 'Apply account lockout policy to WebMail/Admin even when connecting from 127.0.0.1', 'Encrypt login passwords when transmitting over the network', and 'Use the same browser tab for Webmail & Admin pages'. The 'Default folder names' section has three text fields: 'Sent Items folder' (Sent Items), 'Deleted Items folder' (Deleted Items), and 'Drafts folder' (Drafts).

Webmail Advanced Tab

The WebMail Access restrictions tab lets you configure rarely used settings for the WebMail & administration server component of VPOP3.

The **Allow Password in URL** option allows you to create links to Webmail/admin containing the user's password. There is a security risk involved with this, especially if the password is sent in plain text, but some people find it convenient, and it can be useful for automating some administrative processes. To specify the username and password in the URL, add parameters user= and either password= or md5pass= to the URL, e.g. <http://server:5108/admin/index.html?user=postmaster&password=admin> or <http://server:5108/admin/index.html?user=postmaster&md5pass=21232f297a57a5a743894a0e4a801fc3>. The md5pass parameter is an MD5 hex digest (case insensitive) of the password. This helps with hiding the password, but will not prevent replay attacks, and the original password may still be discovered with sufficient resources.

The **Allow different client addresses for a Web Mail session** option means that VPOP3 does not associate a login session with a particular IP address. This makes it more vulnerable to replay attacks, since if someone can capture the session cookie which is being used, that could be used from another computer (until it expires). However, this option is sometimes needed for people accessing the WebMail service from behind a proxy server farm, or other shared address pool (e.g. some mobile phone companies).

The **Support CalDAV scheduling extension** option enables or disables the experimental support for RFC 6638 automatic scheduling extensions to the CalDAV service. This is currently not fully implemented in VPOP3, and it could cause some problems for some CalDAV clients, so you can disable it if you wish or need. If this is disabled then free/busy viewing may not be available in some CalDAV clients.

The **Support different CalDAV authentication realms for different accounts** option makes VPOP3 behave slightly out of the standard and it will request different authentication details for different calendar access. This can help with accessing several accounts from Mozilla Lightning, but can cause issues with other CalDAV clients such as the ones from Apple. We recommend this is turned off unless you need it.

The **Mail HTML Pages** setting tells VPOP3 where to find the content for the WebMail & administration facilities. Usually it will be the `_webmail` folder inside the main VPOP3 installation folder, but there are cases where you may want to change it.

The **Apply account lockout policy to WebMail/Admin even when connecting from 127.0.0.1** option tells VPOP3 to lock accounts if there are too many failed login attempts, even from the VPOP3 computer using the 127.0.0.1 loopback address. We recommend that this is left off all the time, as you may make it impossible to access the VPOP3 settings if you are unsure of the password. If the option is off, then accounts will be locked if they are accessed from other IP addresses, so that will help to protect against remote attacks. If an attacker has access to the VPOP3 computer in order to be able to use the loopback address, then you have bigger issues to worry about!

The **Encrypt login passwords when transmitting over the network** option tells VPOP3 to use a challenge-response MD5 one-way hash of passwords when they are sent over the network from the Webmail login page. This helps to protect against network snooping, and is usually recommended. It is not necessary if you are using [HTTPS encryption](#) of sessions in [VPOP3 Enterprise](#), as all the data is encrypted in that case. Note that if you use this option, then you cannot tell VPOP3 to automatically use Windows passwords when logging into Webmail. The Windows login APIs require VPOP3 to supply the passwords in plain-text, which is not possible if they have been encrypted using a one-way hash.

The **Use the same browser tab for Webmail & Admin pages** option tells VPOP3 to use the same browser window/tab when a user switches between WebMail & Admin modes. Otherwise it will open two different tabs, one for each mode.

The **Default folder names** section lets you specify the WebMail folder names used by default for *Sent Items*, *Deleted Items*, and *Draft* messages. Users can change these folder names afterwards, so these settings will not apply to existing user accounts, but will apply to any new accounts which are created.

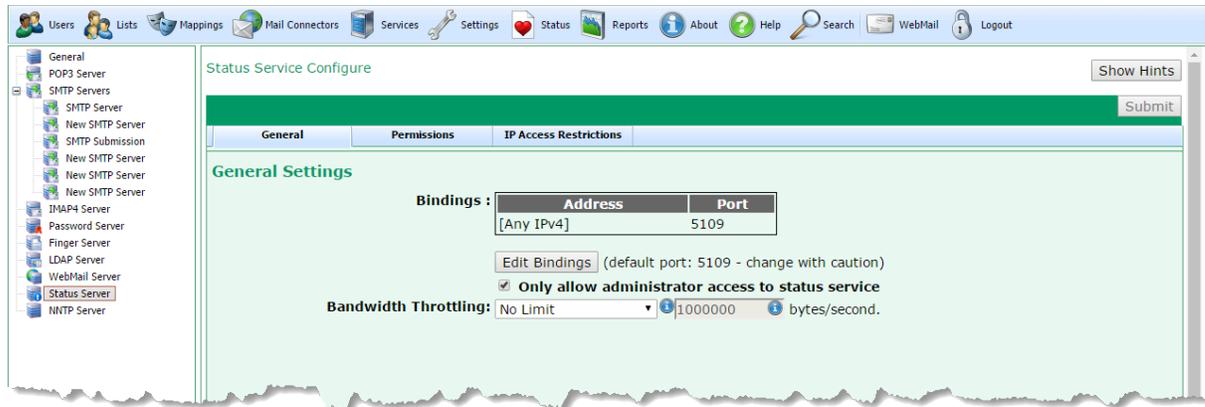
5.5.9 Status

The VPOP3 Status service provides services for the [VPOP3 Status Monitor](#) to be able to access VPOP3.

- [General Tab](#)
- [Permissions Tab](#)
- [IP Access Restrictions Tab](#)

5.5.9.1 General

To get to this page, to to [Services](#) → [Status Server](#) → General



The VPOP3 Status service provides services for the [VPOP3 Status Monitor](#) to be able to access VPOP3.

The **Bindings** section is described in the [Service Bindings](#) topic. If you change the port number, then you must ensure you change the configuration for any VPOP3 Status Monitors which are connecting to this copy of VPOP3.

If the **Only allow administrator access to status service** option is checked, then only VPOP3 administrators can use the VPOP3 Status Monitor.

Bandwidth Throttling allows you to set limits on how fast data will be transferred through this SMTP service. This allows you to prevent it taking up all your available bandwidth. See the [Bandwidth Throttling](#) topic for more information.

5.5.9.2 Permissions

To get to this page, to to [Services](#) → [Status Server](#) → Permissions

The screenshot shows the 'Status Service Configure' interface with the 'Permissions' tab selected. The page title is 'Status Service Configure' and there is a 'Show Hints' button. Below the title bar are tabs for 'General', 'Permissions', and 'IP Access Restrictions'. The 'Permissions' section contains a list of permissions for two groups: Administrators and Non-Administrators. Each permission has a dropdown menu with 'All allowed' selected. Below the permissions is a section titled 'Users' with a note: 'If you click on the icon next to a select box above, the section below will list the users who are allowed to use that option.' The 'Users' section is currently empty.

Permission	Administrators	Non-Administrators
Be able to view Connection Status	All allowed	Mixed
Be able to view Total Queue message counts	All allowed	Mixed
Be able to view User Queue message counts	All allowed	Mixed
Be able to view 'Activity Log'	All allowed	Mixed
Be able to make VPOP3 Connect	All allowed	Mixed
Be able to make VPOP3 shutdown	All allowed	Mixed
Be able to receive Instant Messages	All allowed	Mixed
Be able to send Instant Messages	All allowed	All allowed

Users

If you click on the icon next to a select box above, the section below will list the users who are allowed to use that option.

VPOP3 Enterprise 6.20 - lmail.pcs.co.uk - 192.168.66.23 | Idle | In: 45782 | Out: 1

This page lets you set who can access the various functions of the VPOP3 Status Monitor. On this page you can only set permissions for all administrators or all non-administrators. To set permissions for individual users, go to the [User's Permissions tab](#).

The various permissions are:

- **Be able to view connection status** - the user can see whether VPOP3 is collecting/sending mail or idle, etc.
- **Be able to view total queue message counts** - the user can see the total number of messages waiting in users' inboxes.
- **Be able to view user queue message counts** - the user can see the number of messages waiting in individual users' inboxes.
- **Be able to view 'Activity Log'** - the user can see the details of sending/receiving messages, including who the senders & recipients of messages are.
- **Be able to make VPOP3 connect** - the user can tell VPOP3 to start or stop a connection to send and/or collect messages.
- **Be able to make VPOP3 shutdown** - the user can tell VPOP3 to shutdown or restart (obviously, not recommended for non-administrators!)
- **Be able to receive Instant Messages** - the user can receive basic instant messages from other VPOP3 users through the status monitor.
- **Be able to send Instant Messages** - the user can send instant messages to other VPOP3 users through the status monitor.

For each option you can choose **All allowed** or **All denied** to say that all users of that type are allowed or not allowed that permission. There is also a **Mixed** option which will display if different users of that type have different access to that permission.

If you click the  icon to the right of the drop-down box, the section at the bottom of the page will list the users who are allowed that permission. This is an aid. You cannot alter the users who have the permission through that page: it is read-only.

5.5.9.3 IP Access Restrictions

To get to this page, to to [Services](#) → [Status Server](#) → IP Access Restrictions

This tab is present for all VPOP3's Services. For general details on how this tab works, see the [IP Access Restrictions](#) section.

5.5.10 IP Access Restrictions

Each Service in VPOP3 has an **IP Access Restrictions** tab. This tells VPOP3 which networks/computers can access this part of VPOP3, and, in some cases, which users can access this part of VPOP3 from which computers.

The basic functionality is the same for each service, but different services may be slightly difference. For instance, some services (SMTP and LDAP) can support anonymous usage as well as authenticated usage, so the IP Access Restrictions can be set to indicate which computers can access it anonymously. Other services (eg Finger) do not support authentication, so it is not possible to restrict access by user.

This page will describe the most functional IP Access Restrictions settings, with all the options, but the particular service you are using may not have the **Allow Unauth** or **Users** columns.

Use Global Access Restrictions if more restrictive

Restrict	Type	Address	Prefix	Allow Unauth	Users
Allow	IPv4	12.122.56.77	/32	<input checked="" type="checkbox"/>	<All>
Allow	IPv4	192.168.70.20	/32	<input checked="" type="checkbox"/>	<All>
Allow	IPv4	192.168.70.25	/32	<input checked="" type="checkbox"/>	<All>
Block	Routers			<input type="checkbox"/>	<All>
Allow	IPv4	192.168.66.0	/24	<input checked="" type="checkbox"/>	<All>
Allow	Local Nets			<input type="checkbox"/>	<All>
Block	GeoIP Lookup	RU,CN		<input type="checkbox"/>	<All>
Allow	Any			<input type="checkbox"/>	paul,robot,support,webmaster

Add Remove Defaults

Detected Network Info

- Routers: 192.168.66.1
- Networks: 127.0.0.0/8,192.168.66.0/24,FE80::/64,::1/128

The **Use Global Access Restrictions** option tells VPOP3 to use the Access Restrictions set on the [Global](#) services page as well as the service-specific Access Restrictions. If either will block the connection, then the connection will be blocked. Generally this is turned off because it can cause confusion, but the option is there if you wish to use it.

The restriction table has four or more columns. In this case it has six columns, but the **Allow Unauth** and **Users** columns may not be relevant for the particular service you are configuring.

Restrict - this column tells VPOP3 whether to **Allow** or **Block** connections from the assigned computers.

Type - this indicates how the computers assigned to this rule are defined. These are described below.

Address - this usually indicates the host or network address for this rule.

Prefix - this indicates the CIDR prefix for the network for this rule (eg /24 is equivalent to a subnet mask of 255.255.255.0, /32 is a single IPv4 host, /128 is a single IPv6 host).

Allow Unauth - this indicates whether unauthenticated/anonymous access is allowed from the assigned computers. This option is only available if unauthenticated access is optional for a particular protocol - eg SMTP or LDAP.

Users - this indicates which users are allowed to access from the assigned computers. This defaults to all users. This option is only available when authentication is used for the protocol.

The entries in this table are processed in order from top to bottom, and the first entry which matches is used. Entries are sorted in this table automatically with more specific entries at the top, and less specific ones lower down. Note that when you edit or add a new entry, they are not sorted immediately, but if you reload the page after saving any changes, the sorted order will be displayed.

Type

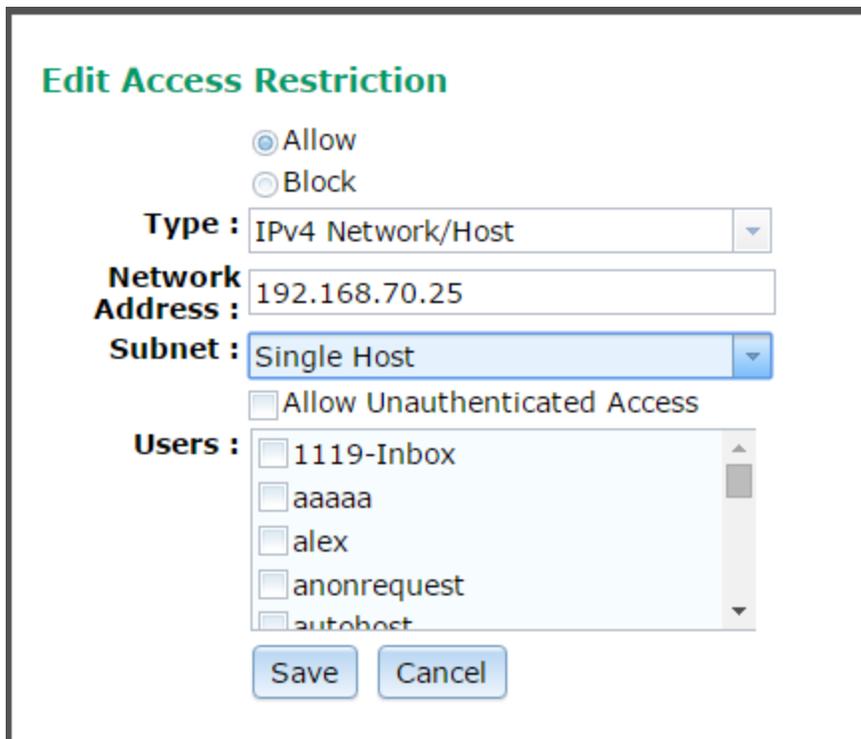
The **Type** column can be:

- **Routers** - this indicates the **Default Gateway** address(es) assigned to this computer. These are detected when VPOP3 starts up. Usually you will block access to these addresses since your router will not want to access your mail or send outgoing mail. Blocking access to your routers will NOT usually block access to remote users (unless your router is acting like a proxy server, which is rare).
- **Local Networks** - this indicates the local network(s) assigned to this computer. These are detected when VPOP3 starts up. The default configuration is that these are allowed. Note that VPOP3 can only detect local networks directly connected to the VPOP3 computer, not other local networks which may be accessed via a local router. The networks detected by VPOP3 are indicated below the access restrictions table in a section titled **Detected Network Info**.
- **IPv4 Network/Host** - this indicates a specified IPv4 network or host.
- **IPv6 Network/Host** - this indicates a specified IPv6 network or host.
- **GeoIP Lookup** - this indicates that the IP address should be looked up in a local database, and then checked against the specified data. Often this is used for blocking IP addresses using geolocation (eg in the above example, connections are not allowed from IP addresses in Russia or China). See the [GeoIP Lookup](#) topic for more information.
- **Any IPv4 Host** - this indicates any IPv4 host.
- **Any IPv6 Host** - this indicates any IPv6 host.
- **Any Host** - this indicates any IPv4 or IPv6 host.

Modifying the Access Restrictions

To add a new restriction, press the **Add** button below the table. To remove one, select it, and press the **Remove** button. The **Defaults** button will remove all entries and replace them with a simple default setting (block routers & allow local networks).

To edit a restriction, double-click it.



Edit Access Restriction

Allow
 Block

Type : IPv4 Network/Host

Network Address : 192.168.70.25

Subnet : Single Host

Allow Unauthenticated Access

Users :

- 1119-Inbox
- aaaaa
- alex
- anonrequest
- autohost

Save Cancel

You can choose all the options here. To select a single computer, type the IP address in the **Network Address** box and choose **Single Host** from the **Subnet** list. To select a network, type the network address (eg **192.168.1.0** in the **Network Address** box), and choose the appropriate subnet mask/CIDR prefix from the **Subnet** list.

Technical Note

Note that the network address is not a valid IP address. For a 255.255.255.0 network, the last number should always be 0. In general, any binary digits (bits) in the network address after the CIDR prefix count are zeros, so in a /24 network (255.255.255.0) and bits after the first 24 bits are zeros, so if an IP address is 192.168.1.57, that is 1100 0000 1010 1000 0000 0001 0011 1001. By setting the bits after the first 24 bits to zeros, you get 1100 0000 1010 1000 0000 0001 0000 0000, which is displayed as 192.168.1.0

If you don't select any users from the Users list, then VPOP3 treats it as if all users have access.

5.5.10.1 GeolIP Lookup

GeolIP lookup in VPOP3's Service [Access Restrictions](#) can be used to specify that only IP addresses from certain countries can access VPOP3 services. Many people use this type of restriction to prevent access from countries commonly used by attackers.

In fact, the VPOP3 GeolIP facility isn't limited to GeolIP data. Essentially it has a database which matches IP address ranges to a 'tag' and then you can check against the tags. A common use would be GeolIP – the tags would be country codes – but it could be used for other things as well. As the database

is queried live, you could even update the database dynamically and have VPOP3 update its access restrictions automatically.

GeolIP database

However, a common use is GeolIP, so that is what this article will describe.

Installing GeolIP data

The first thing is that VPOP3 does not include any GeolIP data. This is partly due to licensing restrictions of such data, and also because it often changes, and there are different sources.

So, to use the GeolIP facility, you need to obtain GeolIP data and import it into VPOP3.

One free GeolIP database source is [GeoLite](#) from [Maxmind](#), so that is what this article will use. You need to decide what sort of data you will be checking against. For this example we will use the **GeoLite Country** database. You can also check against cities, or ASNs (essentially checking against Internet providers' ranges).

For these steps you need the CSV database, so to download the GeoLite Country database, go to <http://dev.maxmind.com/geoip/legacy/geolite/>. At the bottom is a Downloads section, click on the **Download** link in the "CSV/zip" column for **GeoLite Country**. This file is about 1MB. Extract the CSV file from there to a temporary location (eg c:\temp).

If you want, you can open up this file to see what it contains. It will easily open in a text editor, or a spreadsheet program. Each line contains 6 columns. The first two are an IP address range – eg "1.0.0.0" to "1.0.0.255". The second two columns are the same data but as a 32 bit integer rather than dotted IP addresses (it isn't significant how these are calculated as we are going to ignore these). The fifth column contains the ISO country code for the country in question, eg 'AU' for Australia, or 'GB' for the United Kingdom. The sixth (last) column contains the name of the country/region, eg 'Germany' or 'Russian Federation'. For our purposes we'll be using the first two and fifth columns so we can link the IP address range to the country code.

What we need to do is import this data into the VPOP3 database.

We have created a tool you can download to import the data. It's called **VPOP3GeoImport** and it is run from a command prompt. To use it, download the file from <http://www.pscs.co.uk/downloads/vpop3/VPOP3ImportGeoIP.zip> and extract into the VPOP3 installation directory. Then, from a command prompt run it as:

```
VPOP3GeoImport [options] importcsv <filename> 125
```

Normally you won't need any options, but if you run "VPOP3GeoImport -?", you will get a list of options available. (The '125' at the end tells the program which columns to import, in this case, columns 1, 2 and 5).

This program will delete all existing data in the GeolIP database within VPOP3 and then add the data from the CSV file. Note that you do not need to stop VPOP3 while you perform this operation.

Using the GeolIP data

To use the GeolIP data, in the relevant VPOP3 Access Restrictions settings, select the **GeolIP Lookup** type in your access restriction, and enter the desired 'tags' in the **Address** box. In the case of the above country GeolIP data, the tags would be ISO country codes, eg US, GB, etc. To specify multiple tags to look for, you can separate them with commas or semicolons. The Access Restriction rule will match if any of the tags are matched.

Technical

The GeoIP data is stored in a database table called **geoipv4**. This has 4 columns:

- **id** – numeric primary key, assigned by the database
- **addrfrom** – IP address at the start of the range
- **addrto** – IP address at the end of the range
- **result** – the data to be retrieved if the searched IP address is within the range $\text{addrfrom} \leq \text{address} \leq \text{addrto}$

If multiple entries match the searched IP address, then each result will be checked against the specified access restrictions.

5.5.11 Service Bindings

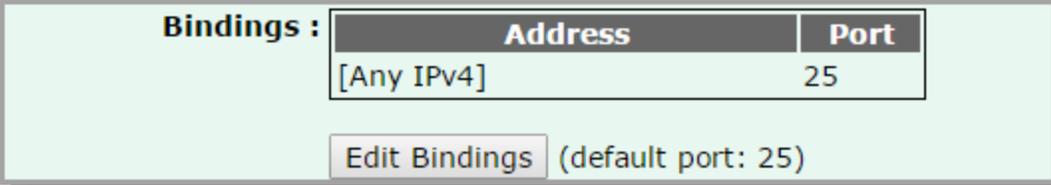
Each service in VPOP3 has 'bindings' which associate an IP address and port number with the service. VPOP3 Basic allows just a single IP address/port for each service, and VPOP3 Enterprise allows an unlimited number of IP address/port combinations for each service.

The bindings say which IP address(es) and port(s) the service is listening on.

For instance, the default for the SMTP service is to listen on port 25 (the standard port for SMTP), on all local IP addresses. If you have another SMTP server on the same computer as VPOP3, they will clash if they both try to listen to port 25 on all IP addresses, so there are two ways you can make them work together - alter the bindings on one or other of the servers so one is listening on a non-standard port, or set up two IP addresses on the computer, and make each service listen on port 25 on a different IP address.

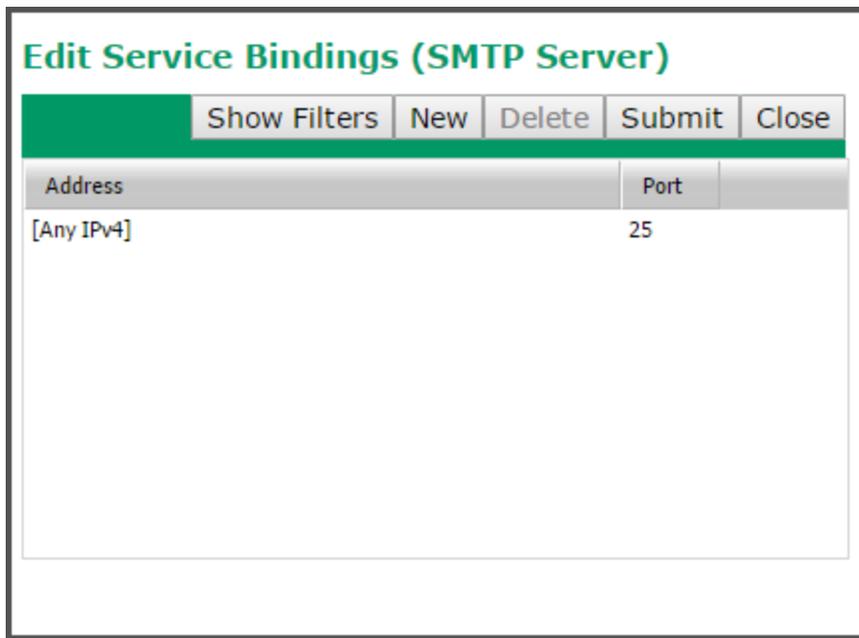
The bindings can be set from the [General Services](#) page, or from the **General** tab in each service's configuration.

In each service's configuration, on the **General** tab there will be a section which looks like this (the address, port and default port values may be different)



Address	Port
[Any IPv4]	25

To edit the bindings, press the **Edit Bindings** button.



To add a binding, press the **New** button, to delete a binding, select it, then press the **Delete** button. To save changes, press the **Submit** button, to close the window without saving changes, press the **Close** button. The **Show Filters** button lets you filter the table entries in to only show a subset.

To edit a binding, you can double-click on the entries in the table.

If you double-click on the entry in the **Address** column, then you will be presented with a list of IP addresses which are available on the VPOP3 computer, as well as **[Any]**, **[Any IPv4]**, and **[Any IPv6]**. If you select any of **Any** options, then VPOP3 will listen on any IP addresses (of the appropriate type) which are unused by any other software and are available on the VPOP3 computer. If the IP addresses change while VPOP3 is running, then VPOP3 will listen on the new set of IP addresses without needing to be restarted.

If you double-click on the entry in the **Port** column, then you can type in the port number which you want VPOP3 to listen on.

VPOP3 will check that the IP address/port combination is not already in use when you make changes. Note that it cannot tell if other software may use the address/port combination in the future or if other software which is not currently running would use the address/port combination, so you should still choose wisely.

5.5.12 Bandwidth Throttling

Each service in VPOP3 can have Bandwidth Throttling enabled. This restricts how much of your connection speed is used by the VPOP3 service.

This may be useful if you have a slow Internet connection and you want to limit VPOP3 so that it does not use all of the available bandwidth.

In VPOP3 Basic, basic bandwidth throttling is available. In [VPOP3 Enterprise](#), there are more options including bandwidth pools to limit several connections' bandwidth usage at once.

For each Service, on the **General** tab there's an option called **Bandwidth Throttling**. This option sets how VPOP3 limits bandwidth usage. The default setting is **No Limit** meaning that bandwidth isn't limited by VPOP3.

In VPOP3 Basic there are two options: **No Limit** and **Custom**. In VPOP3 Enterprise you have those two options as well as **Bandwidth Pool** options.

Let's look at the two basic settings first

No Limit

The **No Limit** option, as the name suggests, means that there is no bandwidth limiting.

Custom

The **Custom** option lets you specify a maximum speed (in bytes/second) for each connection using this service. So, if you set the custom value for the IMAP4 service to 100000, then each connection using the IMAP4 service will be limited to 100,000 bytes per second (800,000 bits per second). If the server is handling 10 IMAP4 connections at once, then each connection is limited to 100,000 bytes per second, so the total throughput could be up to 1,000,000 bytes per second.

For many bandwidth control operations this has limited use, because you may want to throttle the IMAP4 service to only use so much bandwidth regardless of how many connections there are. This is where Bandwidth Pools come into play.

Bandwidth Pools

To have access to Bandwidth Pools, you need to have [VPOP3 Enterprise](#).

Bandwidth pools are configured in Settings → [Misc Settings](#) → [Bandwidth Pools](#). VPOP3 supports 1000 bandwidth pools. By default, they are all configured to allow unlimited bandwidth.

You can easily assign a bandwidth limit to a pool by double-clicking on the 'Allowed Bandwidth' column for the pool you want to edit, and typing in the new bandwidth limit (in bytes per second). You can also assign a name to the bandwidth pool for your future reference.

Misc Settings

ID	Name	Allowed Bandwidth
1	IMAP4	100000
2	pool-2	0
3	pool-3	0
4	pool-4	0
5	pool-5	0

Now, you could go to the IMAP4 service settings, and choose **Bandwidth Pool 1** to be the bandwidth limit for the IMAP4 service. When you have done that, then all the connections using that service will share the bandwidth from the chosen bandwidth pool.

If you wish, you could also choose **Bandwidth Pool 1** to be the bandwidth limit for the POP3 service as well. Now, the bandwidth pool allowance is shared among all POP3 and IMAP4 connections.

Advanced Pools

If you wish, you can create 'nested pools'. To do this, use negative numbers as the pool bandwidth limit where the negative number indicates the 'parent' pool. For instance, you could create settings as below. In this case, the *POP3* and *IMAP4* pools both share the *VPOP3* pool limit. This is achieved by looking at the ID of the *VPOP3* pool (3), and making it negative, and setting that as the limit for the 'child' pools.

Misc Settings

ID	Name	Allowed Bandwidth
1	IMAP4	-3
2	POP3	-3
3	VPOP3	100000
4	pool-4	0
5	pool-5	0

The *POP3* and *IMAP4* pools are not copies of the *VPOP3* pool, but share the pool, so all users of the *POP3* and *IMAP4* pools would be limited to 100,000 bytes per second in total.

In itself this does not give you any functionality you would not otherwise have (you could simply set both the *POP3* and *IMAP4* services to use the *VPOP3* pool), but it does mean that in the future, you could change the limits from the Bandwidth pool settings without having to edit the services individually. This becomes even more useful when you come to use bandwidth scripting,

Bandwidth Scripting

The real power of the bandwidth limits becomes apparent when you can use scripting (only in VPOP3 Enterprise) using the Lua programming language.

The reference guide for the bandwidth scripting is in this article, but here are some examples and ideas. The reason we have used scripting rather than discrete settings is that scripting would allow the feature to be used in ways we may not have considered yet.

Every time a new connection starts to a VPOP3 service, or the 'state' changes (eg someone logs in), then a Lua function is called. This function is called 'GetBandwidth' and is stored in the 'bandwidth.lua' script (managed through the [Scripts](#) settings page). This function is passed several parameters, such as

details of which service the connection is for, user details (if any), client IP address, and so on. Then, the function can return a value to indicate the bandwidth limit to be used:

- 0 = no limit
- 1 to 999999999 = limit for this connection (in bytes per second)
- -1 to -1000 = bandwidth pool to be used (as a negative number – "-1" = bandwidth pool 1, etc)

As you can probably imagine by now, there are many ways this can be used. For instance:

- you could give some people a different bandwidth limit from other people,
- external IP addresses could have a low limit, while internal IP addresses are unlimited,
- you could use other Lua function to do things such as check the current time, and give different bandwidth limits based on the time of day (however, note that the function is only called at the start of the connection, not periodically while the connection is active).

Examples

External IP addresses are limited

```
function GetBandwidth(params)
-- pool '1' is set to the limited pool
-- This function either returns unlimited for local users (192.168.x.y), or '-1' to assign ext
  if string.find(params["clientip"], "^192%.168%.") then
    return 0; -- unlimited
  else
    return -1; -- use pool 1
  end;
end;
```

Most users are limited, but the boss isn't

```
function GetBandwidth(params)
-- pool '1' is set to the limited pool
-- This function either returns unlimited for connections from 'theboss', or '-1' to assign ot
  if params["username"] == "theboss" then
    return 0; -- unlimited
  else
    return -1; -- use pool 1
  end;
end;
```

External IP addresses are limited to different pools depending on time of day. The boss is always unlimited

```
function GetBandwidth(params)
-- pool '1' is set to the daytime limited pool
-- pool '2' is the evening limited pool
-- This function either returns unlimited for local users (192.168.x.y), or the boss, or '-1'
  if string.find(params["clientip"], "^192%.168%.") or params["username"] == "theboss" then
    return 0; -- unlimited
  else -- limited users
    t = os.date("*t");
    if (t.hour >= 18) or (t.hour == 17 and t.min >= 30) or (t.hour < 8) or (t.wday == 6) or (t
      return -2; -- use pool 2 after 5:30pm or before 8am or at weekends
    else
      return -1; -- use pool 1 at other times of day
    end;
end;
```

```
end;  
end;
```

5.6 Settings

On this page, choose an item in the left topic list to configure one of the features of VPOP3. If you are not sure which option to use, using the 'Search' option on the toolbar may help.

- [Admin Settings](#)
- [Anti-virus](#)
- [Attachment Processing](#)
- [Autoresponder Settings](#)
- [Database](#)
- [Diagnostics](#)
- FaxServer
- Global Address Book
- [Global Signature](#)
- [Groups](#)
- [Header Processing](#)
- [Legacy Extensions](#)
- Listserver Settings
- [Local Mail](#)
- [Logging](#)
- [Message Archiving](#)
- [Message Authentication](#)
- [Message Monitoring](#)
- [Misc Settings](#)
- Plugins
- [Quotas](#)
- [Scripts](#)
- [Security Settings](#)
- SMS
- [Spam Filter](#)
- [VPOP3 Text Strings](#)

5.6.1 Admin Settings

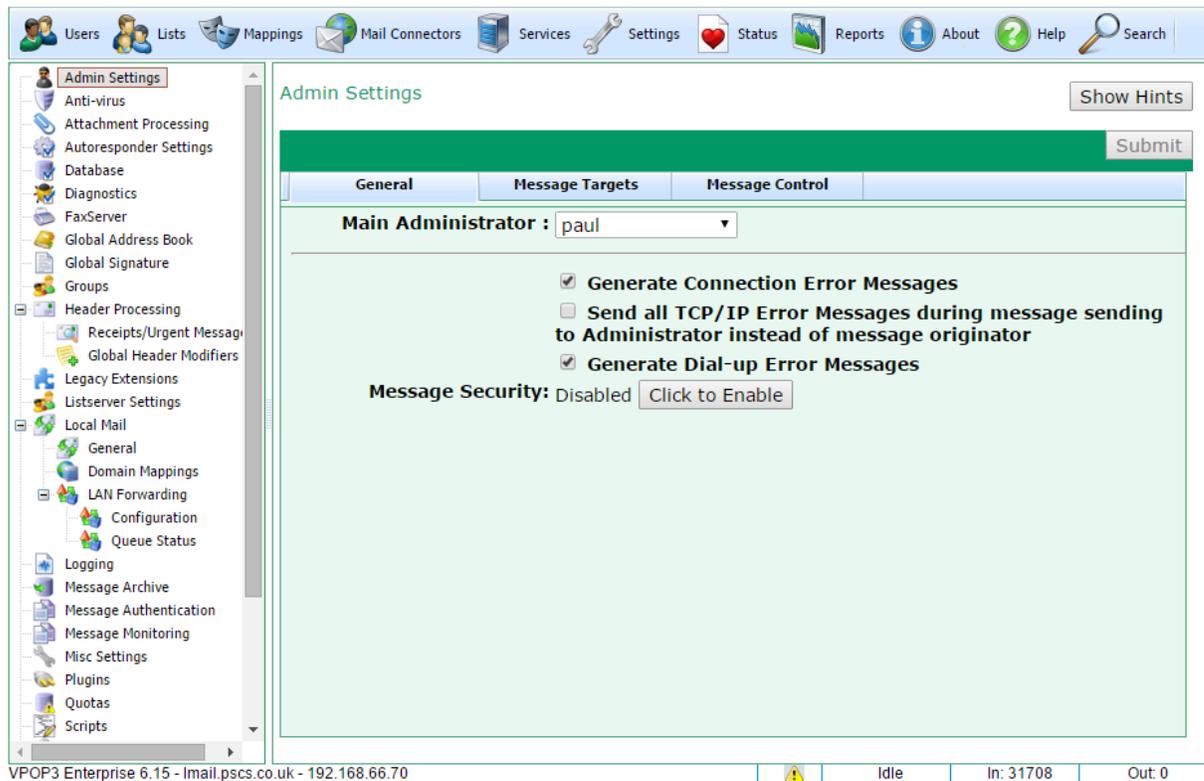
The Anti-virus section allows you configure options for VPOP3's administration behaviour

- [General Tab](#)
- [Message Targets Tab](#)

➤ [Message Control Tab](#)

5.6.1.1 General Tab

To get to this page, go to Settings → Admin Settings → General



This page lets you configure general settings for VPOP3 administration.

The **Main Administrator** is which VPOP3 user will receive error messages from VPOP3 when no other recipient has been specified (eg see the [Message Targets](#) tab). Note that this does not indicate which users can log into the VPOP3 settings as an administrator. That is [configured in the user's settings](#), and is indicated in the [Users list](#) by a 'key' icon to the left of the account name.

The Main Administrator cannot be an external email address, but must be a VPOP3 user. This user can have a [forwarding or assistant address](#) (or addresses) specified if you wish error messages to go to an external email address. However, note that if there is a problem with sending messages out, then VPOP3 will obviously not be able to send the error messages out either in that case.

We *strongly* recommend that the Main Administrator is set to a user who will read their emails. It is very common for people to leave it set to the initial user (eg Postmaster) whose emails are never read, so users are not aware of any problems which are happening.

The **Generate Connection Error Messages** option tells VPOP3 to generate error messages if it cannot connect to a remote mail server for some reason. Usually this will be checked, but you may wish to uncheck it if you want to minimize the number of error messages the Main Administrator receives. Note

that if you do uncheck it, it may not be obvious when VPOP3 has a problem collecting or sending messages.

The **Send all TCP/IP Error Messages during message sending to Administrator instead of message originator** option tells VPOP3 to send error messages to the Main Administrator instead of to the message originator, if VPOP3 has a network problem while sending a message. Choose this option depending on your requirements. If someone is reading the Main Administrator messages, and your users do not understand networking, then it may be more appropriate to check this box so that someone who can understand the error message receives it. Note that this option only affects networking error messages. If the error is something like an unknown recipient, then the error message will always go back to the original message sender.

The **Generate Dial-up Error Messages** option only affects you if VPOP3 has a [dial-up networking connection](#) to the Internet. If it connects through a router, then this option is irrelevant. If this option is checked, then VPOP3 will generate an error email whenever it has a problem making a dial-up connection.

Message Security

The **Message Security** facility should be used with caution!

Message Security tells VPOP3 to disable any functionality which will allow an administrator to access message contents. Note that this does *not* just affect being able to view users' messages via the [Users](#) page, but also prevents them configuring [Mappings](#), setting [assistants](#), enabling [Message Monitoring](#), etc etc. It greatly limits the features that the administrator can access!

Also, note that there is no easy way for an administrator to remove Message Security once it is enabled, without having access to the Message Security Password! (If there was such a way, then the feature would not be much use, as its purpose is to prevent administrators from performing certain tasks.)

To enable message security, click the **Click to Enable** button on this page. You will be prompted to enter, and confirm a password which you are setting for Message Security.

MAKE SURE YOU REMEMBER OR KEEP A COPY OF THIS PASSWORD.

If you forget or lose the password, then you will have to contact VPOP3 technical support for help, and this will often require us to create a 'cracker' program for you to reset the password. This may take some time, and may be chargeable.

Once you have set Message Security, then some features will become inaccessible to administrators, and you will have to enter the password to be able to use those features.

Message Security is intended for the rare cases where people have to be made administrators but are not allowed to access other users' emails.

5.6.1.2 Message Targets

To get to this page, go to Settings → Admin Settings → Message Targets

The screenshot shows the 'Admin Settings' window with the 'Message Targets' tab selected. The 'System Message Targets' section contains a list of message types and their target users:

Message Type	Target User
Antivirus	Main Administrator
AntivirusUpdate	Main Administrator
ArchiveBackup	Main Administrator
Attachments	Main Administrator
Autoresponder	Main Administrator
autoupdate	Main Administrator
BadMailerDaemonMessage	Main Administrator
BadOutqueueFile	Main Administrator
DatabaseBackup	Main Administrator
DownloadRuleAskDefault	Main Administrator
DownloadRuleDelete	Main Administrator
EvaluationExpiry	Main Administrator
Exceptions	Main Administrator
ExternalRouterError	Main Administrator
FaxError	Main Administrator
InvalidRecipient	Main Administrator
LanFwd	Main Administrator
ListServerBadMessageAlert	Main Administrator
MailboxQuota	Main Administrator
MailingList	Main Administrator
MailingListDefaultModerator	Main Administrator
MailingListDefaultOwner	Main Administrator
NntpClient	Main Administrator
OffsiteBackupRestore	Main Administrator
outqueueprocesserror	Main Administrator

The interface also shows a navigation menu on the left, a top toolbar with options like 'Users', 'Lists', 'Mappings', etc., and a status bar at the bottom indicating 'VPOP3 Enterprise 6.15 - lmail.pcs.co.uk - 192.168.66.70'.

This page lets you configure where certain types of error/notification/status messages are sent.

The default is that all messages go to the **Main Administrator** user, set on the [General tab](#). In most cases, this is suitable, but in some larger installations it may not be.

For each type of message, you can choose who the message will go to - either **Main Administrator** if you want the messages to go to whoever the Main Administrator currently is (the default), **<None>** if you want the messages to be simply discarded, or a specific VPOP3 account name.

Some of the types of message targets, with descriptions, are listed below:

- **Antivirus** - if an integrated antivirus solution encounters a problem, this target will receive an email notification containing information on the problem.
- **AntivirusUpdate** - if/when the VPOP3 AV virus definitions are updated, this target will receive an email telling them of the update.
- **ArchiveBackup** - if an ["offline archive backup"](#) is made, this target will receive an email with the results of that backup operation.
- **Attachments** - if an error occurs with [attachment filtering](#), this target will receive a notification email.
- **Autoresponder** - if an error occurs with an [autoresponder](#), this target will receive a notification email.
- **AutoUpdate** - if a VPOP3 automatic update occurs (or fails), this target will receive a notification email.

- **BadMailerDaemonMessage** - if an unrecognised message is sent to the VPOP3 Mailer_Daemon user, then this target will receive a notification email.
- **BadOutqueueFile** - if VPOP3 encounters a bad outqueue message file (eg due to a third party virus scanner corrupting it) then this target will receive a notification email

5.6.1.3 Message Control Tab

To get to this page, go to Settings → Admin Settings → Message Control

The screenshot shows the VPOP3 Admin Settings interface. The left sidebar contains a tree view of settings categories. The main content area is titled 'Admin Settings' and has tabs for 'General', 'Message Targets', and 'Message Control'. The 'Message Control' tab is active, showing 'System Message Repeat Controls'. A text block explains that these controls suppress repeated error messages. A summary states: 'In the past 24 hours 278 Messages have been suppressed by controls.' Below this is a table:

Components	Type	Severity	IDs	Text Search	Forget After	Steps
Misc Component	All	All	Set 1	.*	1440 mins	1:0
Mail Sender	All	All	All	.*	10080 mins	1:0,2:10,3:60,4:1440
Mail Collector	All	All	All	.*	10080 mins	1:0,2:10,3:60,4:1440
All	All	All	0	.*XVZVXVZVZVZ	10080 mins	1:5,3:22
All	All	All	All	.*	1440 mins	1:0,5:10,10:60

Below the table is an 'Add Control' button and the text: 'To edit/delete a control click on the relevant row in the table above'. The status bar at the bottom shows 'VPOP3 Enterprise 6.15 - lmail.pcs.co.uk - 192.168.66.70' and system information like 'Idle', 'In: 32545', and 'Out: 1'.

This page lets you configure how VPOP3 will suppress or allow repeated error messages. This is useful to prevent administrators receiving lots of error messages due to a single problem. However, be careful how it is configured otherwise you may not receive important error messages.

This works by tracking delivered error messages and only sending repeated error messages after a specified amount of time.

The table shows which controls are in place, and which components & types of message they apply to. The default entries are sensible starting options.

To edit or delete a control, click on the row in the table. To add a new control click the **Add Control** button.

Above the table is a count which shows how many messages have been suppressed in the past 24 hours (eg 278 messages in the above screenshot). By clicking on that number, you will be able to view the suppressed messages. This also shows the **Type** and **Severity** of the message in case you want to fine-tune the message controls.

If you edit or add a new control, you will see a window like that below

Edit Administrative Message Control

Component : Mail Collector ▾
Event Type : All ▾
Severity : All ▾
IDs : All ▾
Search Pattern : .*
Forget Previous Messages After : 10080 minutes

Message Alert Steps
 VPOP3 will wait the specified delay before allowing the specified administrative message, or subsequent messages, until a later step applies. The first notification message can also be prevented for a period after the initial error was raised.

To delete a step, clear either box for that step, and save the control.

Step 1 : Message wait minutes after previous message
Step 2 : Message wait minutes after previous message
Step 3 : Message wait minutes after previous message
Step 4 : Message wait minutes after previous message
Step 5 : Message wait minutes after previous message

Component can be **Mail Collector**, **Mail Sender**, **NNTP Collector**, **Misc Component**, **Filtering**, **Routing** or **All**. "Mail Collector", "Mail Sender" and "NNTP Collector" are the components in the **Mail Connectors** section of VPOP3. "Filtering" is attachment or antivirus filtering. Routing is how messages are routed to users' mailboxes. Misc Components are things like fax, backups, mailing lists etc.

If you select the appropriate type in **Component**, then the **IDs** list will be populated with the available options, such as the Mail Sender names, or the various "Misc Components".

In **Misc Components** there are also two options **Set 1** and **Set 2**. **Set 1** is Fax, Archive Backup, Startup and Database Backup. **Set 2** is Mailing Lists, VFX (historical component), OutMail Preprocessor, Logger, Call-Forward Verification, LAN Forwarding, Spam Filter, Recycle Bin.

The **Event Type** is either **Protocol** (e.g. IMAP4, POP3, etc), **TCP/IP** or **Misc**

Severity is **Informational**, **Warning**, **Error**, **Fatal**, or **Panic**. These are different severities of messages, in increasing 'strength'.

The **Search Pattern** is a regular expression to match the error text. .* matches any text.

Forget Previous Messages after X minutes tells VPOP3 how long it should remember previous error messages for.

The various steps tell VPOP3 when to send messages.

In the above example, when a message is generated, VPOP3 will look at how many times this message has been generated in the past 10080 minutes (7 days).

- If this is the first time the message has been generated, then VPOP3 will distribute the message immediately.

- If this is the second time the message has been generated, then VPOP3 will skip distributing the message until at least 10 minutes after the previous message
- If this is the third time the message has been generated, then VPOP3 will skip distributing the message until at least 60 minutes after the previous message

and so on. The final step will repeat forever.

So, as an example, if the message is generated every 7 minutes starting at 12:00, messages will be distributed at 12:00, 12:14 (at least 10 minutes after 12:00), 13:17 (at least 60 minutes after 12:14) and then 13:19 on the following day (at least 1440 minutes after 13:17 on the first day). The messages are not distributed exactly on the 10 minutes because the messages are generated at 12:00, 12:07 (which is suppressed), 12:14 (which is delivered), 12:21 (which is suppressed), etc.

If the steps were as below:

Step 1 : Message <input type="text" value="1"/> wait <input type="text" value="5"/> minutes after previous message
Step 2 : Message <input type="text" value="3"/> wait <input type="text" value="22"/> minutes after previous message

Then the first message to be distributed will be at least 5 minutes after the first message was generated, the second will be at least 5 minutes after that, the third will be at least 22 minutes after that, and then at least 22 minutes after each previous one.

So, if, as before, the message is generated every 7 minutes starting at 12:00, messages will be handled as below:

1. 12:00 - skipped
 2. 12:07 - distributed (at least 5 minutes after the 12:00 one)
 3. 12:14 - distributed (at least 5 minutes after the 12:07 one)
 4. 12:21 - skipped (not 22 minutes after the 12:14 one)
 5. 12:28 - skipped
 6. 12:35 - skipped (only 21 minutes after the 12:14 one)
 7. 12:42 - distributed (at least 22 minutes after 12:14)
 8. 12:49 - skipped
 9. 12:56 - skipped
 10. 13:03 - skipped
 11. 13:10 - distributed
- etc

5.6.2 Anti-virus

The Anti-virus section allows you to set options for VPOP3's integrated virus scanners, such as VPOP3 Antivirus or Sophos SAV Interface.

➤ [General Tab](#)

- [Incoming Messages Tab](#)
- [Outgoing Messages Tab](#)
- [Updates Tab](#)

5.6.2.1 Antivirus General Tab

To get to this page, go to Settings → Anti-virus → General

The screenshot displays the 'Attachment Antivirus Processing' configuration page in the VPOP3 Admin Settings. The interface includes a top navigation bar with icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. A left-hand navigation tree lists various settings categories, with 'Anti-virus' selected. The main content area is titled 'Attachment Antivirus Processing' and features a 'Submit' button in the top right. Below the title is a tabbed interface with 'General', 'Incoming Messages', 'Outgoing Messages', and 'Updates' tabs. The 'General' tab is active, showing the following settings:

- Use **VPOP3 AV** to scan attachments for viruses
- "VPOP3 AV" Version Info**: VPOP3AV Version 1.0.8 AV Database 21060 - Updated Thu Nov 12 17:35:33 2015
Antivirus Subscription Expires: 22 February 2018
Last Antivirus Update: 13 November 2015
- Last 10 items scanned**:

13/11/2015 11:12:11-Scan File	(1) - OK
13/11/2015 11:12:12-Scan File	(0) - OK
13/11/2015 11:12:12-Scan File	(1) - OK
13/11/2015 11:12:12-Scan File	(0) - OK
13/11/2015 11:12:12-Scan File	(1) - OK
- The virus scanner has scanned 16247 files and found 0 viruses since 12/11/2015, 17:22:48.
- Stop accepting messages after a fatal virus scanner error**
Turning this option off could lead to infected messages being delivered to your users if a problem occur with the VPOP3 virus scanner.
- Restart VPOP3 after a fatal virus scanner error**

The status bar at the bottom shows 'VPOP3 Enterprise 6.14 - lmail.pcs.co.uk - 192.168.66.70' and system information: 'Idle | In: 31463 | Out: 0'.

This page lets you configure general settings for how VPOP3 will scan messages for viruses, and shows some status information as well.

The **Use <virus scanner> to scan attachments for viruses** option lets you choose an installed virus scanner to use. Note that here you can only use virus scanners with VPOP3 integration. VPOP3 will not detect other virus scanners on the PC and magically use them for virus scanning. The two virus scanners currently supported with integration are **VPOP3 Antivirus** (based on ClamAV) and **Sophos SAV Interface**.

You install VPOP3 Antivirus by downloading it from our website and installing it on the VPOP3 computer, then restart VPOP3. You install Sophos SAV Interface using the instructions from Sophos.

If you check the checkbox before **Use** then VPOP3 will use the designated virus scanner, and use the drop-down box to choose the desired virus scanner which is installed (if any).

The **Version Info** section shows version information from the virus scanner. The information displayed here depends on the virus scanner in use.

The **Last 10 items scanned** shows the most recent 10 items which the virus scanner has processed, and the results. Note that the virus scanners scans all email sections, not just attachments. If it is a normal email section, then it will show the filename as a number (as in the above screenshot), if it is an attachment, then it will show the attachment name. If the email section/attachment is detected as clean, then it will show 'OK', otherwise it will show error information or the virus detected.

Under the **Last 10 items scanned** box, VPOP3 shows the number of files (or email sections) scanned, how many viruses have been found, and the date VPOP3 was last restarted, which is when the counts apply from.

The **Stop accepting messages after a fatal virus scanner error** option tells VPOP3 that if an unrecoverable error occurs, then VPOP3 should stop accepting messages. This is to prevent messages being received that have not passed through the expected virus scan. This means that if a problem occurs, you will stop receiving messages, and being able to send outgoing messages. Often restarting VPOP3 will fix the problem as it will force the virus scanner to reload, but sometimes it won't. Looking in the **Last 10 items scanned** box should show the errors which are being received.

The **Restart VPOP3 after a fatal virus scanner error** option tells VPOP3 to restart itself if it encounters an unrecoverable virus scanner error. This is an attempt to recover from a problem automatically. However, if the fatal error recurs, VPOP3 will keep restarting, which may cause problems...

5.6.2.2 Antivirus Incoming Messages Tab

To get to this page, go to Settings → Anti-virus → Incoming Messages

The screenshot displays the VPOP3 web interface for configuring antivirus settings. The main content area is titled "Attachment Antivirus Processing" and has a green header with the text "Changes have been made - press: Submit". Below the header are four tabs: "General", "Incoming Messages", "Outgoing Messages", and "Updates". The "Incoming Messages" tab is selected, showing the "Incoming Infected Messages" section. This section includes several options:

- Redirect Infected Messages to:** Postmaster
- Keep a copy of infected attachments in:** c:\vpop3_infected
- Inform sender of infected attachments**
- Totally discard incoming messages containing only viruses whose warnings are to be bypassed**

 A list of viruses to bypass warnings is shown in a scrollable box: Dial/PecDial-B, Mal/Dropper-O, Mal/EncPk-B, Mal/HckPk-A, and Troj/Dorf-*. Below this is the "Email Notifications" section, which includes fields for "Sender:" (empty) and "Reply-To:" (postmaster). The interface also shows a left-hand navigation menu with various settings categories like Admin Settings, Anti-virus, and Spam Filter. The status bar at the bottom indicates "VPOP3 Enterprise 6.14 - Iml.pscs.co.uk - 192.168.66.70" and shows system information like "Idle", "In: 31463", and "Out: 0".

This page lets you configure how VPOP3 deals specifically with virus scanning incoming messages.

The normal behaviour is that if VPOP3 detects a virus, it will remove the infected attachment (or archive, eg ZIP file) from the message, and deliver the remainder of the message to the intended recipients. You can use the options here to alter this behaviour.

Redirect Infected Messages to lets you specify that messages containing infected attachments are redirected to the specified user. Note that the infected attachment or archive is still removed from the message.

Keep a copy of infected attachments in tells VPOP3 to store infected attachments in the specified folder on the server. It is generally not a good idea to enable this option.

Inform sender of infected attachments tells VPOP3 to send a message back to the original message sender if an infected attachment is detected. This can cause backscatter so should be used with caution.

Bypass virus warning for these viruses tells VPOP3 not to send a message back to the original message sender if the virus name (as defined by the AV vendor) matches one of the entries in this list. The list should be specified with one name per line. * and ? wildcards are allowed. For all viruses, simply use * on a line of its own.

Totally discard incoming messages containing only viruses whose warnings are to be bypassed tells VPOP3 that if the incoming message contains only viruses whose names are on the above list, it should discard the message rather than delivering it with the attachments stripped out. This is commonly required nowadays when most email viruses are sent in bulk, rather than legitimate mistakes. If you add a * on a line of its own to the **Bypass virus warnings for these viruses** option, then all messages containing viruses will be discarded silently.

The **Email Notifications** section tells VPOP3 the sender & reply address to use when sending a notification message back to the original message sender (using the **Inform sender of infected attachments** option).

5.6.2.3 Antivirus Outgoing Messages Tab

To get to this page, go to Settings → Anti-virus → Outgoing Messages

The screenshot shows the VPOP3 Administration Console interface. The left sidebar contains a tree view of settings categories, with 'Anti-virus' expanded. The main content area is titled 'Attachment Antivirus Processing' and has a green header bar with the text 'Changes have been made - press: Submit'. Below this is a tabbed interface with 'Outgoing Messages' selected. The 'Outgoing Infected Messages' section contains the following text: 'An attempt to send an infected message will always automatically be blocked at the SMTP level to prevent viruses being sent. You can optionally tell VPOP3 to also tell the administrator when this happened so that they can initiate your virus alert procedure due to the sender's PC being infected.' Below this text is a checkbox labeled 'Inform Main Administrator of Virus' which is currently unchecked. The status bar at the bottom of the window displays 'VPOP3 Enterprise 6.14 - lmail.pcs.co.uk - 192.168.66.70' on the left and 'Idle | In: 31463 | Out: 0' on the right.

This page lets you configure how VPOP3 deals specifically with virus scanning outgoing messages.

VPOP3 will scan outgoing & locally sent messages as well as incoming messages. It will block users from sending messages containing infected attachments. There is no way to disable that behaviour.

The **Inform Main Administrator of Virus** tells VPOP3 to tell the VPOP3 [Main Administrator](#) that someone tried to send a virus, so they can check out that user's computer.

5.6.2.4 Antivirus Updates Tab

To get to this page, go to Settings → Anti-virus → Updates

The screenshot displays the 'Attachment Antivirus Processing' configuration page in VPOP3. The 'Updates' tab is selected, showing the 'VPOP3 Antivirus AutoUpdate' section. A notification at the top states 'Changes have been made - press: Submit'. The settings are as follows:

- Enable AutoUpdate:** (checked)
- HTTP Proxy settings used to download updates (if necessary):**
 - Use HTTP Proxy (it can also use a SOCKS proxy but that is based on the Connection settings)
 - Autodetect proxy settings if possible
- Proxy Server Address:** [Empty text box]
- Proxy Server Port:** 80
- Update Frequency:** 60 minutes

Additional text on the page explains that the Update Frequency is the most frequent that VPOP3 will download updates, and that it will perform the first update on the first connection after startup, then the next update at the next connection that occurs after the 'Update Frequency' amount of time, and so on.

This page lets you configure how VPOP3 updates the virus scanner. This currently only applies to the VPOP3 Antivirus plugin. Sophos SAV Interface is updated using Sophos software, so that is configured from outside of VPOP3.

The **Enable AutoUpdate** option turns on the automatic updates (recommended).

The proxy settings are not used for VPOP3 Antivirus updates. They have been used for other antivirus plugins in the past, but are not used for VPOP3 Antivirus.

The **Update Frequency** tells VPOP3 how often to check for updates. Note that VPOP3 will still only connect according to its [Connection Schedule](#), so if you set this to 60 minutes, but have the Connection Schedule set to every 90 minutes, then VPOP3 will only check for antivirus updates every 90 minutes.

5.6.3 Attachment Processing

The Attachment Processing section allows you to set options for VPOP3 processing attachments, such as filtering attachments, or extracting attachments to a disk directory

➤ [Filtering Tab](#)

➤ [Filtering Conditions Tab](#)

➤ [Extraction Tab](#)

5.6.3.1 Filtering

To get to this page, go to Settings → Attachment Processing → Filtering

The screenshot shows the VPOP3 web interface for configuring attachment filtering. The main section is titled "Attachment Filtering" and contains several sub-sections:

- Attachment filter rules:** A list of rules with their corresponding patterns. The first rule is ".vbs". The second rule is a GUID pattern: "{????????-????-????-??-????????????????}" (with some characters obscured by asterisks in the image). Other rules include ".hta", ".??.???", and a rule for 10 consecutive spaces: "* * * * *".
- Last 10 attachments blocked:** A list of blocked attachments, including files like "20:43:14 - Bill_439087821422735.docm" and "20:41:08 - Bill_01596387.docm".
- Incoming messages:** A section with checkboxes for actions like "Check incoming attachments", "Remove filtered attachments from message", "Change filtered attachment extension to make it unrunnable", "Redirect messages with filtered attachment to:", "Let message through unchanged", and "Delete message".
- Outgoing messages:** A section with a checkbox for "Reject outgoing messages with filtered attachments".
- Email Notifications:** A section for configuring notifications about blocked attachments, including fields for "Sender" and "Reply-To".

This page lets you configure how VPOP3 will filtering incoming and locally sent attachments. This screenshot is from VPOP3 v6.20. Earlier versions did not have some of the options or facilities listed here.

The **Attachment filenames to filter** section lets you select which attachments are to be filtered. Prior to VPOP3 v6.9 this could only contain file names (including DOS style wildcards - ? and *), with one name on a line. In version 6.9 we added the facility for more [flexible advanced conditions](#).

The default filter patterns are:

Pattern	Explanation
*.vbs	Files with a .vbs extension will typically run as Visual Basic Scripts.
* {????????-????-????-??-????????????????}	Filenames ending in a GUID (Globally Unique Identifier) - These files could instruct Windows to open the file in a particular program, or as an executable, irrespective of the actual filename extension. Note: GUIDs only contain hexadecimal characters (numbers 0-9 and letters A-F), but this pattern would also match for non-hexadecimal characters.
*.hta	Files with a .hta extension will typically run as HTML applications; potentially allowing the use of JScript and VBScript.
*.????.???	Files with a 'double' filename extension are commonly used to distract the recipient. For example, by naming a file photo.jpg.exe, the sender could exploit users who do not have the technical knowledge to realise that the file is an application and not a picture.
* * * * *	Files with at least 10 consecutive spaces in the filename. There are few legitimate reasons for using 10 consecutive spaces, so it is likely to be an

Pattern	Explanation
	exploit attempt. Using a lot of spaces may obscure the filename extension in some mail clients, or may make the attachment look like two distinct files.
*.	Windows will disregard the dot at the end of a filename, so there is very little reason for a filename legitimately ending with a dot. An attacker may try using a dot at the end of the filename, in order to circumvent other filtering rules.
*.pif	Files with a .pif extension will typically be Program Information Files for Windows. They can be used to transmit viruses.

The **Filter attachments in ZIP files** option tells VPOP3 to look for the filter patterns inside ZIP files. If you use the advanced filtering condition rules, you can override this setting for each rule if you wish.

The **Block password protected ZIP files** option tells VPOP3 to block any ZIP files which are password protected - this is because these are often used to bypass virus scanners, which cannot scan files inside protected ZIP files. If you use the advanced filtering condition rules, you can specify different filtering conditions for protected ZIP files if you wish.

Last 10 attachments blocked

In VPOP3 v6.16 and later there is a **Last 10 attachments blocked** section which contains the times and filenames of the last 10 attachments blocked by the attachment filter.

In parentheses after the filename is more information. This is:

1. Reason Blocked (eg **BlockAttachments** or **BlockAttachmentsInZip**)
2. Type of message (**SMTPLOCAL**, **SMTPINCOMING** or **POP3**)
3. Sender email address
4. Rule name (this will be the line number of the rule for a basic rule, or the **RuleName** attribute of an advanced rule).

Note that 'BlockAttachments' doesn't mean that the attachment was blocked, just that the filter saw it - if the filter action is to rename attachments, then the attachments will have been renamed even though this displays 'BlockAttachments'.

Incoming Messages

The **Check Incoming attachments** option turns on attachment filtering for incoming messages (both [POP3](#) and [SMTP](#) incoming). If this option is unchecked, then the remainder of this section's options are disabled.

The next set of radio buttons let you choose what happens if VPOP3 detects a prohibited attachment:

- **Remove filtered attachments from message** - if this option is chosen, then VPOP3 will remove the prohibited attachment from the message, and deliver the remainder of the message on to the recipient. VPOP3 will attempt to add text to the message to indicate that an attachment has been removed. In a few cases it may not be possible to add this text, for instance if the message was in a non-standard format. Note that if this option is chosen, and the filtered attachment is inside a ZIP or TNEF (Winmail.dat) archive, then the whole archive will be removed.
- **Change filtered attachment extension to make it unrunnable** - if this option is chosen, then VPOP3 will rename the prohibited attachment by replacing the last character of the extension to a '_' character. For instance, 'document.pdf.exe' will be renamed to 'document.pdf.ex_'. This will usually mean that the user cannot simply click on the attachment to run it, but they must save it to disk,

rename it, and then open it. Hopefully this will give the user time to think and consider whether the document is something they expect and is safe, while still allowing them to receive attachments which have been filtered. Note that if the filtered attachment is in a ZIP file, then the whole ZIP file is renamed. If it is inside a TNEF (Winmail.dat) file, then the TNEF file will be removed, as there is no safe way to rename one so that it will not be opened automatically by Microsoft Outlook.

- **Redirect messages with filtered attachment to:** - if this option is chosen, VPOP3 will redirect any message containing a prohibited attachment to the specified user. Ideally, that user should be able to judge whether the attachment is safe or not (and virus scan it if appropriate), and decide what to do with it.
- **Let message through unchanged** - if this option is chosen, then the message is let through unchanged. This option is not recommended.
- **Delete message** - if this option is chosen, then the message is deleted without informing the local recipient (if the 'Inform sender' options below are selected, then those will still be processed).

Spamfilter Score - if the message is allowed through - e.g. with renamed attachments, redirected or just allowed through unchanged, then the message will have the specified score added to the spamfilter score. This can be used to quarantine the message. For instance, on a default installation, setting this to '100' will mean that any messages with filtered attachments will be put into the spamfilter quarantine. This can be overridden for [specific advanced checks](#).

The **Reject incoming SMTP messages containing filtered attachments** option causes VPOP3's SMTP service to issue an SMTP reject error if it detects a filtered attachment in an incoming message. This should cause the sender of the message to receive an error message from their mail server (or their ISP's mail server). This option overrides the above selection when processing incoming SMTP messages.

The **Inform sender that attachments were filtered - incoming POP3 messages** option tells VPOP3 to send a message to the sender of messages which were received via POP3, if they contain a filtered attachment. This may allow the sender to resend the message with a different file name or via an alternative means. Note that if the attachment filtering blocks attachments containing viruses, the returned messages may cause email backscatter because the sender's email address could have been forged.

The **Inform sender that attachments were filtered - incoming SMTP messages** option tells VPOP3 to send a message to the sender of incoming messages which were received via SMTP, if they contain a filtered attachment. This may allow the sender to resend the message with a different file name or via an alternative means. Note that if the attachment filtering blocks attachments containing viruses, the returned messages may cause email backscatter because the sender's email address could have been forged. It could be more appropriate to use the **Reject incoming SMTP messages** option above.

Outgoing Messages

The **Reject outgoing messages with filtered attachments** option causes VPOP3's SMTP service to issue an SMTP reject error if it detects a filtered attachment in a locally sent message. This should cause the sender of the message to receive an error message in their email client as soon as they send it.

VPOP3 will block the outgoing message with an error like:

```
554 5.7.1 Message prohibited (PROHIBITED FILENAME - <filename>)
```

Email Notifications

If you have enabled either of the **Inform sender that attachments were filtered** options, then the message which VPOP3 sends will have the sender details specified in this section. This should allow the original message sender to reply to the notification message to contact someone who will be able to tell them why the attachment wasn't allowed.

5.6.3.1.1 Attachment Processing Advanced Filter Rules

In the Attachment Processing → [Filtering](#) settings, you can specify rules to indicate which attachments should be filtered.

Starting in VPOP3 version 6.9, you can specify much more advanced rules to be more specific about which attachments are to be blocked. This section describes the advanced rule syntax. Note that because this is a powerful configuration language, it may be complex to understand. The Attachment filter rules section can contain a mixture of plain wildcard filenames, and advanced rules. VPOP3 will process them in order, from top to bottom, until it finds a rule which matches.

An example of an advanced rule is:

```
{
#this rule checks for some HTML files inside ZIP files
  rulename my first attachment filter
  checkzip yes
  checknotzip no
  size < 1kb
  size >= 500
  filename extensions htm html
  content text ajax-loader
}
```

This rule will check for .HTM or .HTML files within ZIP files (but not outside of ZIP files), which are between 500 and 1023 bytes (inclusive) in size, and contain the text 'ajax-loader'.

General syntax rules:

- The start of an advanced rule is indicated by having a { character on a line of its own.
- The rule ends when VPOP3 sees a } character on a line of its own.
- You cannot nest rules.
- The rule can contain actions and conditions. Note that you can have multiple conditions of the same type, and VPOP3 will check them all.
- VPOP3 processes the rule definition in order from top to bottom. Usually this doesn't matter, but in some cases it may - (eg "CheckZip Yes" followed by "CheckEncryptedZip No")
- All the conditions have to match for the rule to match.
- Each action or condition has to be on a line of its own.
- The action/condition name and options are case insensitive. The data is case sensitive except for filename checks which are case insensitive or where specified below.
- The action/condition name must be followed by a space.
- Comments are indicated by lines beginning with a # character

- Spaces at the start or end of the line are trimmed before processing
- Text strings can contain \-escaped text (ie \n becomes a line-feed, \t becomes a tab character, \\ becomes \, \x41 becomes A etc)
- [Regular expressions](#) should be surrounded by / characters and have options after the terminating / character (eg **/word/i**)
- [wildcardpatterns](#) are NOT substring matches. They must match entirely. So, if you want them to be a substring match, surround them with * characters - ie don't just use *fred*, use **fred**.

Variables

Advanced rules have very basic support for variables (to pass data between rules). Variable names cannot contain spaces.

Variables last for the lifetime of processing the current message, so can be used to pass variables between the checks for different attachments within a single message (eg to check for multiple attachments).

Default Variables

When a rule is processed, some variables are set to values which may be useful

\${attachname} contains the name of the attachment currently being processed.

\${archivename} contains the name of the attachment ZIP currently being processed (this is empty if the file being checked is not inside a ZIP file).

\${mimetype} contains the MIME type of the attachment currently being processed as specified in the email message (this is empty if the file being checked is inside a ZIP file).

\${messagetype} contains the 'type' of message currently being processed (SMTPINCOMING, SMTPLOCAL or POP3).

Rule Actions

In the syntax definitions below **bold** characters indicate text you should type as-is, *italics* indicate text you should replace with your own values. (x | y) indicates options, [xx] indicates optional text.

Rulename

Syntax: **Rulename** *rulename*

Example: **Rulename This is my rule**

This specifies a name for the rule. This is used in logging, and can be used the **Log** action. If you do not specify a rule name, then the line number of the start of the rule in the filter list is used.

SetIfMatch

Sets/clears/updates a variable if the rule matches. Note that if the rule matches and any **SetIfMatch** actions are in the rule, then the rule will *not* trigger the 'prohibited attachment' action.

Syntax: **SetIfMatch** *variablename* **Clear**

Example: **SetIfMatch myvar Clear**

Clears the specified variable if the rule matches

Syntax: **SetIfMatch** *variablename* **Set** (*data* | "*data*")

Example: **SetIfMatch myvar Set "This is some data "**

Sets the specified variable to the specified data if the rule matches. Quotes around the data are optional, and will be removed if they are there. If you need to set leading or trailing spaces in the variable, then you should use quotes to avoid them being trimmed. *data* can contain expansions (see below).

Syntax: **SetIfMatch** *variablename* **Append** (*data* | "*data*")

Example: **SetIfMatch myvar Append bible**

Adds the specified data to the specified variable if the rule matches. Quotes around the data are optional, and will be removed if they are there. If you need to set leading or trailing spaces in the variable, then you should use quotes to avoid them being trimmed. *data* can contain expansions (see below).

Syntax: **SetIfMatch** *variablename* **Replace** (*data1* | "*data1*") (*data2* | "*data2*")

Example: **SetIfMatch myvar Replace "some words" "some more words"**

Replaces data in the specified variable if the rule matches. The text in *data1* (case insensitive) is replaced with the text in *data2*. Quotes around the data are optional, and will be removed if they are there. If you need to set spaces in *data1* or you need to set leading or trailing spaces in *data2*, then you should use quotes. *data2* can contain expansions (see below).

Syntax: **SetIfMatch** *variablename* **RegexReplace** (*data1* | "*data1*") (*data2* | "*data2*")

Example: **SetIfMatch myvar RegexReplace "/(some|a few|d+) cats/i" "\1 dogs"**

Replaces data in the specified variable if the rule matches. The regular expression *data1* is replaced with the text in *data2*. Quotes around the data are optional, and will be removed if they are there. If you need to set spaces in *data1* or you need to set leading or trailing spaces in *data2*, then you should use quotes.

You can use \1, \2 etc in *data2* which will be replaced with the contents of the corresponding capture group from *data1*.

SetIfNoMatch

This sets/clears/updates a variable if the rule *does not* match. Other than that, it is the same as the **SetIfMatch** action above.

Syntax: **SetIfNoMatch** *variablename* **Clear**

Syntax: **SetIfNoMatch** *variablename* **Set** (*data* | "*data*")

Syntax: **SetIfNoMatch** *variablename* **Append** (*data* | "*data*")

Syntax: **SetIfNoMatch** *variablename* **Replace** (*data1* | "*data1*") (*data2* | "*data2*")

Syntax: **SetIfNoMatch** *variablename* **RegexReplace** (*data1* | "*data1*") (*data2* | "*data2*")

Log

This causes VPOP3 to write an entry to the VPOP3.LOG file for diagnostic purposes.

Stop

Syntax: **Stop**

Example: **Stop**

This stops the remainder of the attachment filter process if the rule matches. The rule will *not* trigger the 'prohibited attachment' action. This can be useful for preventing attachment filtering in some cases.

SpamScore

(Version 6.20 or later)

Syntax: **SpamScore** *number*

Example: **SpamScore 200**

This adds the specified number onto the spamfilter score which may affect message quarantining (note that *number* can be negative if you wish to use it as a 'whitelisting' mechanism).

Text Expansions

Some actions will expand text strings to include variables. To indicate a text expansion use `${}` around a variable name. Eg `${myvar}` will be replaced with the contents of the **myvar** variable.

Rule Conditions

CheckZip

Syntax: **CheckZip** (**yes** | **no** | **true** | **false** | **1** | **0**)

Example: **CheckZip no**

This tells VPOP3 whether to check inside ZIP files. By default, VPOP3 will check inside ZIP files if the [Filter attachments in ZIP files](#) option is checked, and not otherwise, but this can be specified on a per-rule basis with the advanced rules. This implies both the **CheckEncryptedZip** and **CheckUnencryptedZip** options below.

CheckEncryptedZip

Syntax: **CheckEncryptedZip** (**yes** | **no** | **true** | **false** | **1** | **0**)

Example: **CheckEncryptedZip yes**

This tells VPOP3 whether to check inside encrypted ZIP files. By default, VPOP3 will check inside all ZIP files if the [Filter attachments in ZIP files](#) option is checked, and not otherwise, but this can be specified on a per-rule basis with the advanced rules. Note that the *content* of encrypted ZIP files cannot be tested, but the filenames and compressed & uncompressed sizes can be tested.

CheckUnencryptedZip

Syntax: **CheckUnencryptedZip** (**yes** | **no** | **true** | **false** | **1** | **0**)

Example: **CheckUnencryptedZip 1**

This tells VPOP3 whether to check inside unencrypted ZIP files. By default, VPOP3 will check inside all ZIP files if the [Filter attachments in ZIP files](#) option is checked, and not otherwise, but this can be specified on a per-rule basis with the advanced rules.

CheckNotZip

Syntax: **CheckNotZip** (**yes** | **no** | **true** | **false** | **1** | **0**)

Example: **CheckNotZip 0**

This tells VPOP3 whether to check files which are not inside ZIP files. By default, VPOP3 will check these files, but you can turn it off on a per-rule basis if you wish.

Size

Syntax: **Size** (< | > | <= | >= | <> | != | == | = | **ne** | **eq** | **le** | **lt** | **ge** | **gt**) [*number* { (**kB** | **MB**) }

Example: **Size >100MB**

This compares the size (uncompressed size) of the attachment as specified.

CompressedSize

Syntax: **CompressedSize** (< | > | <= | >= | <> | != | == | = | **ne** | **eq** | **le** | **lt** | **ge** | **gt**) [*number* { (**kB** | **MB**) }

Example: **CompressedSize lt 57kb**

This compares the compressed size of the attachment as specified. (If the attachment is not in a ZIP file, then the compressed size is the same as the uncompressed size.)

Filename / Name

This checks the filename of the attachment as specified. **Filename** and **Name** are equivalent.

Syntax: **Filename** [**not**] **text** wildcardpattern

Example: **Filename text *.exe**

This checks the filename against the wildcard pattern specified. If **not** is used, then the check will match if the filename does *not* match the pattern. The wildcard pattern can include DOS style wildcards (* & ?).

Syntax: **Filename** [**not**] **regex** *regex*

Example: **Filename not regex /\.exe\$/i**

This checks the filename against the [regular expression](#) specified. If **not** is used, then the check will match if the filename does *not* match the pattern.

Syntax: **Filename** [**not**] **extensions** *ext* [*ext...*]

Example: **Filename extensions html htm js**

This checks the filename against the list of extensions specified (1 or more). If the extension matches any of the specified extensions, then the check will match. If **not** is used, then the check result is inverted.

Variable / Var

This checks the contents of the specified variable. **Variable** and **Var** are equivalent.

Syntax: **Variable** *variablename* [**not**] **text** *wildcardpattern*

Example: **Variable myvar not text aaaaa***

The specified variable's contents will be compared against the wildcard pattern specified. If **not** is used, then the check will match if the variable contents do not match the pattern. The wildcard pattern can include DOS style wildcards (* & ?).

Syntax: **Variable** *variablename* [**not**] **regex** *regex*

This checks the specified variable's contents against the [regular expression](#) specified. If **not** is used, then the check will match if the variable contents do *not* match the pattern.

Content

This checks the content of the attachment as specified. The contents of files inside encrypted ZIP files cannot be checked. Also, VPOP3 will only allow you to check attachments up to 100kB in size (for performance reasons). Content checks have optional start/end/length settings to allow you to limit which part of the attachment to check. The start & end default to the start and end of the attachment. You can use either end or length as you wish.

Syntax: **Content** [**start** *startpos*][(**end** *endpos* | **length** *length*)] [**not**] **md5** *md5hexdigest*

Example: **Content start 1000 length 1000 md5 ea231b125002c3212d3278deff2f1152**

Calculates the MD5 hash of the attachment (or specified portion of the attachment) and compares the hex digest to the specified value.

Syntax: **Content** [**start** *startpos*][(**end** *endpos* | **length** *length*)] [**not**] **text** *text*

Example: **Content end 1234 text hello**

Searches for the specified text (case sensitive) in the attachment

Syntax: **Content** [**start** *startpos*][(**end** *endpos* | **length** *length*)] [**not**] **base64** *base64encoded*

Example: **Content start 1000 end 2000 base64 aGVsbG8=**

Searches for the specified base64 encoded data in the attachment

Syntax: **Content** [**start** *startpos*][(**end** *endpos* | **length** *length*)] [**not**] **hex** *hexbytes*

Example: **Content not hex 68 65 6c6c6f**

Searches for the specified hex encoded data in the attachment

Syntax: **Content** [**start** *startpos*][(**end** *endpos* | **length** *length*)] [**not**] **regex** *regex*

Example: **Content regex \b(hello|hi)\b/i**

Searches for the specified regular expression in the attachment

Header

This checks the contents of the specified message header field.

Syntax: **Header** *headerfield* [**not**] **text** *wildcardpattern*

Example: **Header subject not text aaaaa***

The specified header field will be compared against the wildcard pattern specified. The wildcard pattern can include DOS style wildcards (* & ?).

Syntax: **Header** *headerfield* [**not**] **regex** *regex*

Example: **Header from regex /<[^>]+@gmail\.com>/i**

This checks the specified header field against the [regular expression](#) specified.

5.6.3.2 Filtering Conditions

To get to this page, go to Settings → Attachment Processing → Filtering Conditions

The screenshot shows the 'Attachment Processing' configuration page in VPOP3. The 'Filtering Conditions' tab is active. The page title is 'Attachment Filtering Conditions'. Below the title, there is a text block explaining the filter syntax: 'These filters are specified as <Header field> ":" <Data to match>', with examples like 'Subject: don't filter*' and 'Subject: /nos+filter/'. There are two main sections for defining filters:

- Skip filtering for :** A text box containing 'From: *customer.com*'. To the right, it says: 'If the message headers match any of these headers, then the attachment filtering will be skipped.'
- Do filtering for :** An empty text box. To the right, it says: 'If this is not blank, and the message header match any of these headers, then the attachment filtering will be used, unless the message also matches a 'skip filtering' condition. If this is blank, then VPOP3 will filter all messages unless they match a 'skip filtering' condition.'

The status bar at the bottom of the window displays: 'VPOP3 Enterprise 6.14 - I-mail.pcs.co.uk - 192.168.66.70'.

This page lets you tell VPOP3 to skip [attachment filtering](#) for some messages, or to only do it for some messages.

The **Skip Filtering** and **Do Filtering** boxes let you specify message header conditions. When a message is received, VPOP3 looks at the message headers and tries to match them against these conditions. It processes them as follows:

1. If any message headers match any of the **Skip Filtering** conditions, then the attachment filtering will not be performed, otherwise
2. If the **Do Filtering** condition list is empty, the attachment filtering will be performed, otherwise
3. If any message headers match any of the **Do Filtering** conditions, then attachment filtering will be performed, otherwise
4. Attachment filtering will not be performed

The conditions are specified as **<header field> : <data to match>**

The <header field> is any message header field (as defined in RFC 5322 or any custom fields). If you view the message source in your email client you will see the message headers at the start of the message. Common ones to check for are **To, Cc, From, Subject**.

The <data to match> is text to match, DOS wildcards are allowed (* and ?)

So, an example may be:

```
From: *@customer.com*
```

This will match any message where the From: address contains @customer.com anywhere in the header field.

Note that the matching is simple matching. For instance, if you are matching the From address, VPOP3 does not parse the header and only check the actual email address, it just looks at the raw content of the From header field. Many times there is extra information around the actual email address, for instance the From header field may actually look like:

```
From: Joe Brown <joe.b@company.com>
```

So, that is why we used wildcards in the example, because we don't know whether there will be any data after the end of the email address. If you look at the message headers of received messages that you want to check for, you may be able to be more precise in the text to match.

5.6.3.3 Extraction

To get to this page, go to Settings → Attachment Processing → Extraction

This page lets you tell VPOP3 to extract attachments in incoming messages into files on disk. This screenshot is from VPOP3 v6.20. Earlier versions did not have some of the options or facilities listed here.

Attachment extraction does not affect outgoing or internal messages.

If the **Extract attachments to directory** checkbox is checked, then VPOP3 will copy all attachments on incoming messages to the specified directory.

The directory specification tells VPOP3 where to store the attachments. The default is `%base%_attach`. `%base%` gets converted to the VPOP3 installation directory, so the default is the `_attach` subdirectory of the VPOP3 installation directory.

You can specify text which will be expanded out to dynamic data to allow the attachments to be sorted as you wish.

The available expansions are:

- **%subject%** - this gets converted into the incoming message's subject
- **%sender%** - this gets converted into the incoming message's sender's email address (in v6.20 and later)
- **%recipient%** - this gets converted into the message's recipient email address (in v6.20 and later). If the message had multiple recipients, then the attachments will be saved multiple times on disk
- **%year%**, **%month%**, **%day%**, **%hour%**, **%minute%** - these will be replaced by the appropriate numeric value
- **%dow%** - this gets converted to a number for the current day-of-week (0 is Sunday, 6 is Saturday)

- **%date%** - this gets converted to the current in the local format.

Any expansions are made filename safe - so invalid characters are converted into `_` characters.

If the **Leave attachments in the original message** option is checked, the original message is left untouched. Otherwise it is replaced with a link/reference to the extracted attachment. (Whether this link is usable will depend on the path you specify and the receiving user's share/file permissions. VPOP3 doesn't enforce this).

If the **Put attachments in subdirectories by message subject** option is checked, then this is equivalent to adding `\%subject%` to end of the specified directory.

If the **Put attachments in subdirectories by receipt date** option is checked, then this is equivalent to adding `\%date%` to the end of the specified directory.

If the **Resolve filename conflicts** option is checked, then any duplicate filenames will be replaced with `Copy_<n>_of_<filename>`. If the option is not checked, then files will be overwritten.

Attachment extraction can be modified using Lua scripting - see [our knowledgebase](#) for details.

5.6.4 Autoresponder Settings

To get to this page, go to Settings → Autoresponder Settings

Autoresponder Settings
Show Hints

Standard Subject Prefix for autoresponses :

Make autoresponders conform to RFC 3834 (recommended)

Return path for autoresponses :

Precedence header for autoresponses :

Autoresponder header filters :
(specify header fields & values to search for. If these headers exist, the autoresponder will not trigger. Wildcards (* and ?) can be used)

Precedence: Bulk
 Precedence: List
 X-Spam: *
 List-: *

Autoresponder reply filters :
(specify email addresses to reply to or not reply to. Use ! at the start of a line to indicate that this address should not be replied to. Wildcards (* and ?) can be used. Any addresses which do not match a filter rule will be replied to by the autoresponder)

!Mailer*Daemon@*
 !*-request@*
 !owner.-*@*

Autoresponder Templates

Autoresponder templates let an administrator create an autoresponder definition which users can then choose when creating their own autoresponder

Autoresponder Templates :

This page sets global settings defining how autoresponders in your VPOP3 installation work. To configure autoresponders or "out-of-office replies" for specific users, [edit the user](#), and go to the [Autoresponder](#) tab in their settings.

[RFC 3834](#) is a document specifying recommended behaviour for automatic response to emails. By default VPOP3 follows the recommendations in this document.

The **Standard Subject Prefix for autoresponses** indicates text which will be added to the beginning of the subject of the automated responses. RFC 3834 says that subject lines should contain an indication that it is an automatic response, and suggests "Auto:" as a possible indication. You can override this or remove it as you wish. Note that individual autoresponder configurations can override it on an individual basis as well. The setting here is used if the individual autoresponder configurations are left at the default settings.

The **Make autoresponders confirm to RFC 3834** option tells VPOP3 to behave as required by the recommendations. There is usually no need to turn this off. The differences in behaviour are that if this box is checked:

- VPOP3 will add a **References:** and an **In-Reply-To:** message header containing the Message-Id of the original message
- VPOP3 will add a header line saying **Auto-submitted: auto-replied**
- VPOP3 will send the automated reply to the **Return-Path** of the original message, rather than the **Reply-To** address (RFC 3834 section 4 requires this, and explicitly says not to use the Reply-To address. This is because if you are a member of a mailing list, messages to the Reply-To address will usually be distributed to everyone on the mailing list, which is not desirable)
- If a Reply-To address is not explicitly specified in the autoresponder definition, VPOP3 will set it to **no-one@<your domain>**. This will make any emails which come in reply to your autoresponse (eg other automated responses) be discarded.

The **Return path for autoresponses** setting lets you specify where bounce messages caused by the autoresponder messages will be sent. The default is <blank> which means that bounce messages will not be generated. This is usually the correct thing to do because you do not generally want to receive bounce messages caused by autoresponder messages failing to be delivered. If you want, you can specify an alternate email address for the bounce messages to go. This email address *must not* have an autoresponse configured on it, itself, otherwise you may create a mail loop between the autoresponder and the bounce message generator.

The **Precedence header for autoresponses** setting lets you set the value of the Precedence header field in the automated responses. The Precedence header is non-standard, but many people use it, and like to set automated responses to have a specific value, such as 'bulk'. This can help to prevent mailing loops.

The **Autoresponder header filters** box lets you specify data to look for in the message header of the incoming message. If any headers match, then the autoreponse will not be triggered. VPOP3 will also not respond if the incoming message contains an **Auto-submitted** header field with any value other than **No**. The standard header filters will prevent automated responses to bulk or list messages and many other autoresponder messages.

For example: **Precedence: Bulk** looks for the **Precedence:** line in the message header and checks if the data for that header field is **Bulk**. VPOP3 does a case-insensitive check and allows [wildcards](#).

The **Autoresponder reply filters** box let you specify email addresses that autoresponders should or should not be replied to. The default has some sensible examples. You may want to use this to only automatically reply to certain addresses, in that case you could specify something like ***@example.com**, or you could use this option not to send automated replies to messages from local users, in that case you could specify something like **!*@mycompany.com**.

Autoresponder Templates

The **Autoresponder Templates** section lets you create autoresponder definitions which all users can use when configuring their own autoresponders.

In the **Autoresponder Templates** drop-down either choose an existing template and press **Edit** or choose the **<New>** entry to create a new autoresponder template. See the [Edit Autoresponder Definition](#) topic for instructions on creating an autoresponder definition.

5.6.5 Database

The Database Settings allows access to settings & utilities related to the back-end database used by VPOP3 and the email message store

- [Backups Tab](#)
- [Query Tab](#)
- [Connection Tab](#)
- [Message Store Tab](#)
- [Offsite Backup Tab](#)
- [Restore Tab](#)

VPOP3 uses a [PostgreSQL database server](#) for storing configuration and message data. Without access to this database, VPOP3 cannot do anything, so will refuse to start, or will stop if it loses connection to the database.

5.6.5.1 Backups

To get to this page, go to Settings → [Database](#) → Backups

The screenshot shows the 'Database Backups' configuration page. It includes a 'Show Hints' button and a 'Submit' button. The page is divided into several sections:

- PostgreSQL Binary Directory:** c:\vpop3\pgsql\bin
- Backup Command Options:** -F c
- Backup Target File:** DBBack-%w.dmp. A note below explains the format: (Use %h=hour(0-23) %w=weekday(0-6), %d=day of month(1-31), %m=month(1-12), %y=year(4 digits), %2-%9=cycle files N times). It also notes that UNC paths should be used for network locations.
- Target File Network Username:** (empty)
- Target File Network Password:** (empty)
- Verify Network Login Details:** (button)
- Temporary Filename:** (empty)
- Backup Command Sample:** "c:\vpop3\pgsql\bin\pg_dump.exe" -F c -h localhost -p 5433 -U vpop3 -f DBBack-%w.dmp vpop3
- Enable daily database backups:** . A note states: "We strongly recommend you leave this checked unless you have an alternative PostgreSQL backup system in place. A normal disk backup is **NOT** adequate."
- When to backup database:** 1
- Command to run after backup:** (empty)
- Backup database Now:** (button)
- Send 'database backup successful' email messages to administrator:**

This page lets you configure how VPOP3 makes its daily backups. We recommend that you backup the VPOP3 database regularly, and keep a few backups safe in case corruption causes the most recent backup to be unusable. VPOP3 uses PostgreSQL's [pg_dump](#) program to make a backup of the database. There are alternative methods of backing up the database, see the [PostgreSQL documentation](#), or [Blog](#) and our [knowledgebase](#) for some ideas

The **PostgreSQL binary directory** setting lets you specify where VPOP3 can find the *pg_dump* program. Normally this is set correctly to the VPOP3\pgsql\bin folder, but you may have installed PostgreSQL separately in a different directory/drive, so you can specify the location of the program files here.

The **Backup command options** tell VPOP3 which options to specify to the *pg_dump* program. See the [pg_dump documentation](#) for details on the available options. The default is **-F c** which tells *pg_dump* to create a single file containing a compressed backup of the database. This is suitable for local storage. If you are going to store the backups elsewhere you may want to use an uncompressed format (eg **-F c -Z 0** or **-F p**) so that a "delta backup" system can just backup the changed portions of the backup, but you should test these thoroughly before relying on them.

The **Backup target file** tells VPOP3 where to store the backup. VPOP3 creates the backup as a temporary file first. Then, if the backup succeeds, it will copy it to the file name and location that you specify here. As well as specifying the filename, you can specify the directory. As described on this page, you can use replacements to alter the file path/name dynamically - **%h** will be replaced with the hour at the start of the backup, **%w** will be replaced with the week-day number (0=Sunday, 1=Monday, etc), **%d** will be replaced with the day of month, **%m** will be replaced with the month, **%y** will be replaced with the 4 digit year number, and **%2, %3, %4, %5, %6, %7, %8, %9** will be replaced with a number which cycles daily from 0 to n-1 - eg **%5** will cycle through 0, 1, 2, 3, and 4.

For instance, **f:\vpop3backups-%m\back-%3.dmp** will put the backups in folders **f:\vpop3backups-1** to **f:\vpop3backups-12** depending on the month, and store the latest 3 backups for each month in those folders called **back-0.dmp**, **back-1.dmp** and **back-2.dmp**.

If you want to store the backups on a network share, you **MUST** specify the path as a UNC - eg **\\server\share\path**. Mapped drives will not work, because VPOP3 runs as a Windows service, and Windows services do not have access to mapped drives. Also, you will probably need to enter the **Target file network username** and **Target file network password** settings which should specify an account which can access the network share. Because VPOP3 runs as a service it does not have the same login credentials as the currently logged in Windows user. The **Verify network login details** button lets you check that the username and password allow access to the backup location.

The **Temporary filename** lets you specify where VPOP3 stores the temporary backup file it creates before it moves it to the final location. If you leave this blank, the default of **DBBACK.TMP** in the VPOP3 directory is used. This filename *must* be on the same computer as VPOP3, and the VPOP3 account (usually **LocalSystem**) *must* have access to the location. If not, then the backups will fail.

The **Backup command sample** is a read-only field which contains an example command line to make a backup using the specified settings. If you wish, you could copy that line to make a backup manually (or using Windows Task Scheduler, etc), but you may have to change the output filename slightly as that may include % characters which may upset things.

The **Enable daily database backups** box lets you enable or disable the database backups. We strongly recommend that you leave this enabled, unless you have an alternative backup scheme in place which you have tested thoroughly. Note that a simple 'copy' backup of the VPOP3 folders is *not* sufficient, and will almost certainly not be usable.

The **When to backup database** box lets you specify when VPOP3 should run the backups. Enter the hours in here where the backups should start, separated by spaces. For instance **"1 13"** will start a backup at 1am and another at 1pm. In VPOP3 v6.9 and later you can also optionally specify the day-of-week and minutes portion of the time. Indicate the day-of-week by preceding the hour with the day of week (1=Sunday, 2=Monday... 7=Saturday) followed by a '/' character. Indicate the minute by following the hour with a ':' character and the minutes value. For instance **"4/17:32"** means that a backup will be started at 5:32pm on Wednesdays. Multiple times can be specified by separating them with spaces.

The **Command to run after backup** box lets you specify a program to run after the backup has completed. This could copy it somewhere else, send notifications, use a program such as RDIFF to create a delta backup, etc. The command line entered can use the same text replacements as the Backup target file (above), as well as **%f** which gets replaced with the final filename of the backup.

The **Backup database now** button tells VPOP3 to run a backup immediately.

The **Send 'database backup successful' email messages to administrator** option tells VPOP3 to send an email message to the VPOP3 [main administrator](#) when a backup is successfully made. An email is always sent if the backup fails, regardless of whether this option is checked or not.

5.6.5.2 Query

To get to this page, go to Settings → [Database](#) → Query

This page lets you configure how VPOP3 makes its daily backups. We recommend that you backup the VPOP3 database regularly, and keep a few backups safe in case corruption causes the most recent backup to be unusable. VPOP3 uses PostgreSQL's [pg_dump](#) program to make a backup of the database. There are alternative methods of backing up the database, see the [PostgreSQL documentation](#), or [Blog](#) and our [knowledgebase](#) for some ideas

The **PostgreSQL binary directory** setting lets you specify where VPOP3 can find the *pg_dump* program. Normally this is set correctly to the VPOP3\pgsql\bin folder, but you may have installed PostgreSQL separately in a different directory/drive, so you can specify the location of the program files here.

The **Backup command options** tell VPOP3 which options to specify to the *pg_dump* program. See the [pg_dump documentation](#) for details on the available options. The default is **-F c** which tells *pg_dump* to create a single file containing a compressed backup of the database. This is suitable for local storage. If you are going to store the backups elsewhere you may want to use an uncompressed format (eg **-F c -Z 0** or **-F p**) so that a "delta backup" system can just backup the changed portions of the backup, but you should test these thoroughly before relying on them.

The **Backup target file** tells VPOP3 where to store the backup. VPOP3 creates the backup as a temporary file first. Then, if the backup succeeds, it will copy it to the file name and location that you specify here. As well as specifying the filename, you can specify the directory. As described on this page, you can use replacements to alter the file path/name dynamically - **%h** will be replaced with the hour at the start of the backup, **%w** will be replaced with the week-day number (0=Sunday, 1=Monday, etc), **%d** will be replaced with the day of month, **%m** will be replaced with the month, **%y** will be replaced

with the 4 digit year number, and %2, %3, %4, %5, %6, %7, %8, %9 will be replaced with a number which cycles daily from 0 to n-1 - eg %5 will cycle through 0, 1, 2, 3, and 4.

For instance, **f:\vpop3backups-%m\back-%3.dmp** will put the backups in folders **f:\vpop3backups-1** to **f:\vpop3backups-12** depending on the month, and store the latest 3 backups for each month in those folders called **back-0.dmp**, **back-1.dmp** and **back-2.dmp**.

If you want to store the backups on a network share, you MUST specify the path as a UNC - eg **\\server\share\path**. Mapped drives will not work, because VPOP3 runs as a Windows service, and Windows services do not have access to mapped drives. Also, you will probably need to enter the **Target file network username** and **Target file network password** settings which should specify an account which can access the network share. Because VPOP3 runs as a service it does not have the same login credentials as the currently logged in Windows user. The **Verify network login details** button lets you check that the username and password allow access to the backup location.

The **Temporary filename** lets you specify where VPOP3 stores the temporary backup file it creates before it moves it to the final location. If you leave this blank, the default of **DBBACK.TMP** in the VPOP3 directory is used. This filename *must* be on the same computer as VPOP3, and the VPOP3 account (usually **LocalSystem**) *must* have access to the location. If not, then the backups will fail.

The **Backup command sample** is a read-only field which contains an example command line to make a backup using the specified settings. If you wish, you could copy that line to make a backup manually (or using Windows Task Scheduler, etc), but you may have to change the output filename slightly as that may include % characters which may upset things.

The **Enable daily database backups** box lets you enable or disable the database backups. We strongly recommend that you leave this enabled, unless you have an alternative backup scheme in place which you have tested thoroughly. Note that a simple 'copy' backup of the VPOP3 folders is *not* sufficient, and will almost certainly not be usable.

The **When to backup database** box lets you specify when VPOP3 should run the backups. Enter the hours in here where the backups should start, separated by spaces. For instance **"1 13"** will start a backup at 1am and another at 1pm. In VPOP3 v6.9 and later you can also optionally specify the day-of-week and minutes portion of the time. Indicate the day-of-week by preceding the hour with the day of week (1=Sunday, 2=Monday... 7=Saturday) followed by a '/' character. Indicate the minute by following the hour with a ':' character and the minutes value. For instance **"4/17:32"** means that a backup will be started at 5:32pm on Wednesdays. Multiple times can be specified by separating them with spaces.

The **Command to run after backup** box lets you specify a program to run after the backup has completed. This could copy it somewhere else, send notifications, use a program such as RDIFF to create a delta backup, etc. The command line entered can use the same text replacements as the Backup target file (above), as well as **%f** which gets replaced with the final filename of the backup.

The **Backup database now** button tells VPOP3 to run a backup immediately.

The **Send 'database backup successful' email messages to administrator** option tells VPOP3 to send an email message to the VPOP3 [main administrator](#) when a backup is successfully made. An email is always sent if the backup fails, regardless of whether this option is checked or not.

5.6.5.3 Connection

To get to this page, go to Settings → [Database](#) → Connection

This page lets you configure how VPOP3 connects to the PostgreSQL database server. It is rare that you will need to change these options, and if you do you must restart VPOP3 for them to take effect.

Note that these settings are different from other VPOP3 settings in that they are stored in a file called [VPOP3.INI](#) in the VPOP3 installation directory. If you need to change the database connection settings when VPOP3 is not running you can edit that file directly using any plain-text editor, such as Notepad.

- **Database Name** - the PostgreSQL database name that VPOP3 is to use (the default is 'vpop3').
- **PostgreSQL Hostname** - use this setting if VPOP3 is to connect to PostgreSQL using a host name (eg 'localhost' or 'db.example.com') instead of an IP address.
- **PostgreSQL Host Address** - use this setting if VPOP3 is to connect to PostgreSQL using an IP address (IPv4 or IPv6 are allowed - eg 127.0.0.1 or ::1).
- **PostgreSQL Port** - use this setting to tell VPOP3 which TCP port PostgreSQL is listening on. The default is usually 5433. PostgreSQL's default port is 5432, but VPOP3 doesn't use that to avoid conflicting with any other PostgreSQL software on the same computer - the installer finds the first free port higher than 5432, which is usually 5433.
- **PostgreSQL User Name** - the username used to log into PostgreSQL to access the specified database (the default is 'vpop3').

- **PostgreSQL Password** - the password used to log into the specified user in PostgreSQL (the default is 'vpop3pass').
- **Connection Timeout** - how many seconds VPOP3 will wait for a connection to the PostgreSQL server to be established (default is 0 - wait indefinitely).

VPOP3 uses a 'connection pool' to connect to PostgreSQL. Establishing a connection to the server can be slow, so once VPOP3 has made a connection and finished with it, rather than releasing the connection, it puts it into a 'pool' where future connection requests can reuse it rather than having to establish a new connection. If the connection in the pool is not used for a long time, VPOP3 will close it. Each connection to PostgreSQL will create a new 'postgres.exe' process which can be seen in Windows Task Manager. The default PostgreSQL connection allows up to 100 connections at once, but several are needed for system purposes.

- **Max Connections** - the maximum number of connections normally allowed in the connection pool.
- **Absolute Max Connections** - if VPOP3 needs a connection and there are no free connections in the pool, it will wait for a few seconds and then make an extra connection up to the **Absolute Max Connections** limit. (If it needs further connections after that, then it will wait indefinitely for one to become available). If VPOP3 has to make connections like this it usually indicates a performance or overloading problem on the server.
- **PostgreSQL service** - usually blank and rarely used - [see the PostgreSQL documentation](#)

Below this are counts showing how many connections are currently in use and how many are currently in the connection pool. This should normally be below the **Max Connections** limit above. In the above screenshot, there are 14 connections in the connection pool, 5 of which are being used (9 are unused and available instantly if needed).

5.6.5.4 Message Store

To get to this page, go to Settings → [Database](#) -> Message Store

Database
Show Hints

Backups

Query

Connection

Message Store

Offsite Backup

Restore

Message Store

Delay while moving messages : ms

When VPOP3 v2 or earlier is initially upgraded to v3 or later, VPOP3 moves messages from the old message store to the new database store. To reduce load on the server, it does this slowly. Reduce this number to increase this speed (and increase server load).
0 message summaries queued to be imported into the DB
0 message contents queued to be moved into the DB
VPOP3 will only start moving messages once the relevant mailbox/folder is accessed. One of the folders with pending messages is

Message Recycle Bin

Message Recycle Bin : Keep deleted messages in a 'recycle bin' for hours
(set to 0 to disable recycle bin)

Recycle Bin Size : 956 message(s) in existing folders (21.09 MB)
0 message(s) in 0 deleted folder(s) (0 bytes)

Message Store Stats

Message Data: In Database: 412589 (13449MB) - In Files: 0 (0B)
Folders: Num folders: 651 - Most Messages: 57139 - Biggest: 1938MB - Most Unread: 44968
Messages: Total Messages: 417253 - Total Size: 13594MB - Total Unread: 201114

Global Prune Rules

Folder	Age	Size	Read	Flagged	Deleted	Spam

VPOP3 v2 and earlier stored messages as individual files. VPOP3 v3 and later store messages in the [PostgreSQL database](#). If you upgrade VPOP3 from v1 or v2 to a later version, VPOP3 will move the data from the old individual files into the database. It does this in the background, so that the upgrade process does not take an excessive amount of time. The messages will still be accessible whichever form they are in.

The **Delay while moving messages** sets how long VPOP3 waits between moving each message to the new database message store. Because the messages are accessible in the old v1/v2 form as well, this is not treated as an urgent process, so the delay defaults to 1 second to minimise the load on the server. If you have a reason to speed this up, you can decrease this number, but this will increase the server load.

Below this setting is some information about messages & folders which are still needed to be transferred into the new database form. In an established VPOP3 v3 or later installation, these numbers should all be zero.

Message Recycle Bin

VPOP3 Enterprise Only

VPOP3 Enterprise has a Message recycle bin where messages are stored after the user deletes them. This allows for easy recovery of accidentally deleted messages via the user's [Advanced tab](#) in their settings. Here you can set how long VPOP3 will keep messages in the recycle bin. The default is 72 hours (3 days). If you set this to 0 then the recycle bin function is disabled.

The **Purge recycle bin** button lets you empty the recycle bin now (this action is not reversible). Usually you would not do this, but if you have deleted a huge number of emails you may wish to do this to reduce the database size (note that it will not reduce the disk space used by the database, but will reduce backup sizes, and further actions can be carried out to reduce the used disk space)

The **Recycle bin size** data shows you the amount of messages and total size of messages currently in the recycle bin

Message Store Stats

The Message Store Stats let you see some key information about the message store:

- the total number of messages stored in the database and their total size. Also, the number of messages stored in files in the VPOP3_messages folder tree, and their size (in VPOP3 v3 and v4 and following an upgrade from those versions)
- The number of folders, and the folders with the most messages, most total size and most unread messages. Hovering over the green numbers in this line will show you the 10 highest ranked folders in these categories in case you want to reduce the sizes. Note that we recommend that regularly used folders (eg Inbox, Sent Items, etc) should be kept below 10,000 messages or so to avoid adverse performance. Less commonly used folders may be OK at larger sizes, but if not, this facility lets you see the largest folders.
- The number of messages in folders, their total size and the number of unread messages.

Note that the number of messages and total size of messages in folders and the number of messages and total size of messages stored in the database will rarely match. This is because:

- a) When messages are deleted from folders, VPOP3 will store them in the recycle bin for some time, and then delete them from the database as a background task. This means that the *Message Data* values may be greater than the *Messages* values.
- b) If you copy a message to another folder, VPOP3 will often only store the message content once, but it will be referred to from two folders. This means that the *Messages* values may be greater than the *Message Data* values.

Global Prune Rules



VPOP3 Enterprise

The following option is only available in the [Enterprise edition](#) of VPOP3.

VPOP3 Enterprise can automatically delete messages from folders based on 'Prune rules' which you specify. This section lets you specify the Prune Rules which apply to all users. Each User has their own ['Prune rules'](#) settings as well.

To add a rule, press the **Add Rule** button. To remove one, select it, then press the **Delete Rule** button.

- The **Folder** column indicates the folder for the rule to act on. Use * to mean all folders
- The Age column indicates the age of messages which should be deleted - eg 365 will delete messages over 365 days old.
- The Size column indicates the size of messages which should be deleted (blank means any size)
- The Read column indicates whether read messages should be deleted (can be set to Read, Unread or Either)
- The Flagged column indicates whether flagged (starred) messages should be deleted (can be set to Flagged, Unflagged or Either)

- The Deleted column indicates whether only IMAP4 deleted messages should be (really) deleted, or all messages. If this is checked, the prune rule will *only* delete messages which have been marked as IMAP4 deleted.
- The Spam column indicates whether only messages which VPOP3 detected as spam should be deleted, or all messages. If this is checked, the prune rule will *only* delete messages which VPOP3 detected as spam.

All conditions must match for a message to be deleted. Deleted messages are put into the Message Recycle Bin so can be undeleted if you get the Prune Rule wrong and discover it in time.

For instance, you could set:

- Folder = *
- Age = 30
- Size = <blank>
- Read = Either
- Flagged = Either
- Deleted = checked
- Spam = unchecked

This will really delete (IMAP 'purge') all messages which have been marked as deleted in an IMAP client after 30 days. This can be useful if you have an email client such as older versions of Microsoft Outlook which does not handle IMAP4 deleted messages very well.

A common problem is due to people leaving the **Deleted** and **Spam** checkboxes checked. When adding a new rule, VPOP3 checks these boxes for the new rule to make it unlikely to delete any wanted messages, but if you leave the boxes checked, then VPOP3 will *only* delete messages which were both marked as spam by the spamfilter, and messages which have been marked as IMAP4 deleted already. It will not delete messages which the user has not marked for deletion.

5.6.5.5 Amazon S3 Backup

To get to this page, go to Settings → [Database](#) -> Offsite Backup

Database Show Hints Submit

Message Store Search Index **Amazon S3 Backup** Restore Offsite Backup

Amazon S3 Backup

VPOP3 Enterprise can backup messages to an [Amazon S3](#) data store. In the case of a disaster you will be able to make a new VPOP3 PC recover messages from the Amazon S3 store. This recovery can run while the new VPOP3 server is in use, so you will be able to get back to work more quickly.

Amazon S3 Access Key :

Amazon S3 Secret Key :

Amazon S3 Bucket :

Note that if you change the Encryption Key or Compression setting below, then VPOP3 will have to restart the backup process, so we don't recommend you do this once the backup is established. Note that the encryption key is not recoverable if you lose it!

Compress messages before uploading.

Encryption Key :

Save Settings

Upload messages to Amazon S3 bucket if created or modified by this VPOP3 server.

Download messages from Amazon S3 bucket if uploaded or modified by a different VPOP3 server.

Current state : Waiting

Upload status : OK
Last upload: 2016-10-07 09:16:47 (4 uploaded, 0 deleted)

	On Amazon S3 Server	Pending Upload
Messages	523,234 (17GB)	0 (0B)

Download status : Idle
Last download: 2015-12-17 15:58:11 (0 messages, 0 flags)
Last refresh - 2015-12-17 15:52:55 : 460662 on server
460639 in sync, 0 deleted, 0 pending messages, 0 pending flags
Next refresh - 2015-12-17 16:52:55

VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 Idle | In: 39745 | Out: 1

The Amazon S3 Backup settings let VPOP3 upload messages to the Amazon S3 storage service. VPOP3 uploads message and message status changes as they occur, and it only needs to upload changes, rather than being a full backup just once a day as the local backup facility is. However, the Offsite Backup is purely for messages. Users, Mappings and other settings are not backed up using this facility. Because the S3 service does not know about VPOP3 and is just a plain file store (unlike our [Offsite Backup service](#)), certain things involve more data transfer, for instance moving messages may require messages to be uploaded again using the S3 service, but not using our Offsite Backup service.

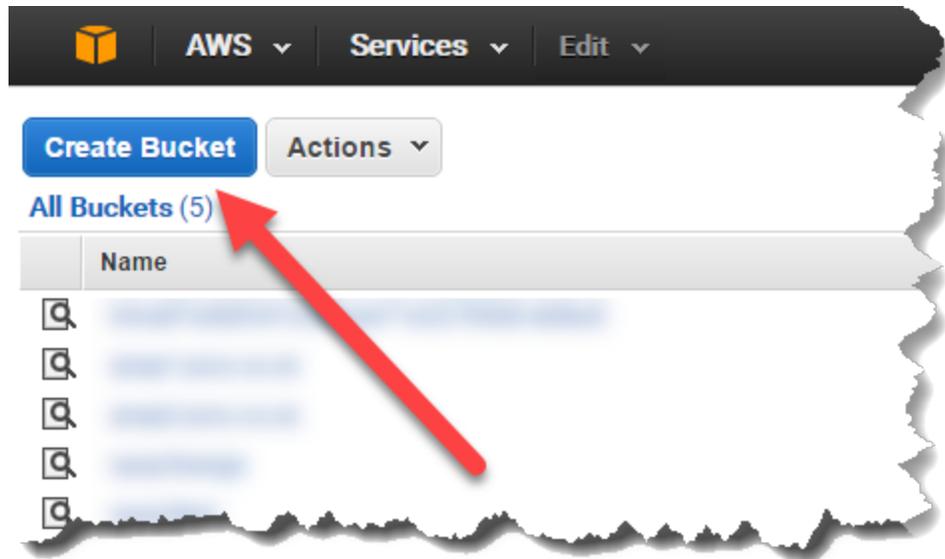
If the VPOP3 server PC fails, you can install VPOP3 on a new PC, and put in the same Amazon S3 details and have VPOP3 download them to the new server.

To use this facility, you need to have an [Amazon S3 account](#) and create a 'bucket' for the backup to be stored in (we recommend that you *do not* use a bucket used for any other purpose).

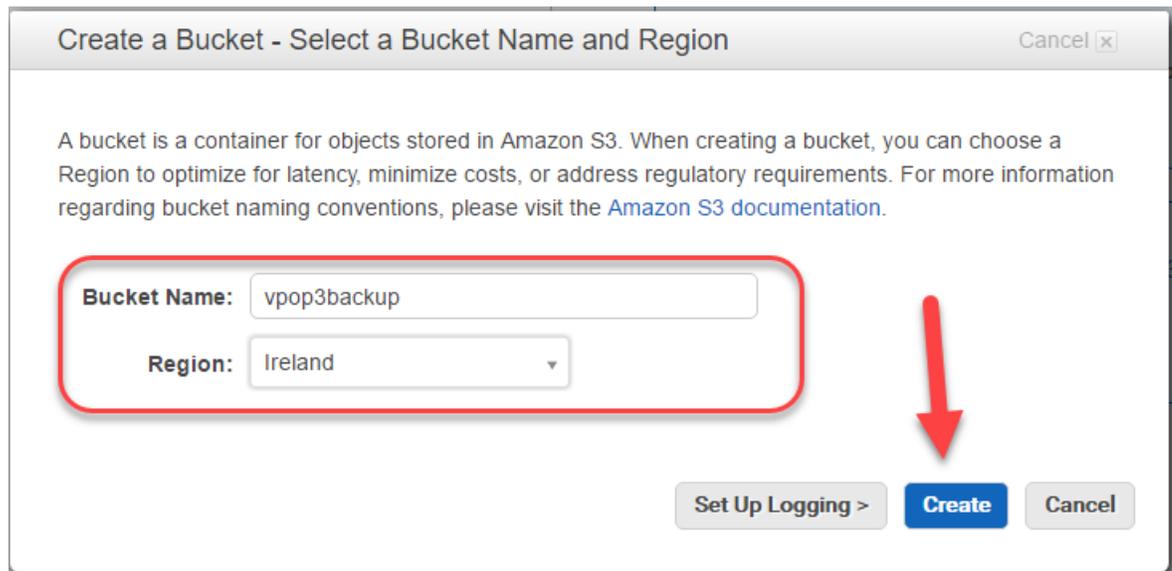
- Create an Amazon S3 Bucket and security credentials

Log into Amazon AWS at <https://aws.amazon.com/> (create an Amazon account if necessary), then go to Services -> S3 to access your Amazon S3 control panel.

Create a new 'Bucket' in S3.

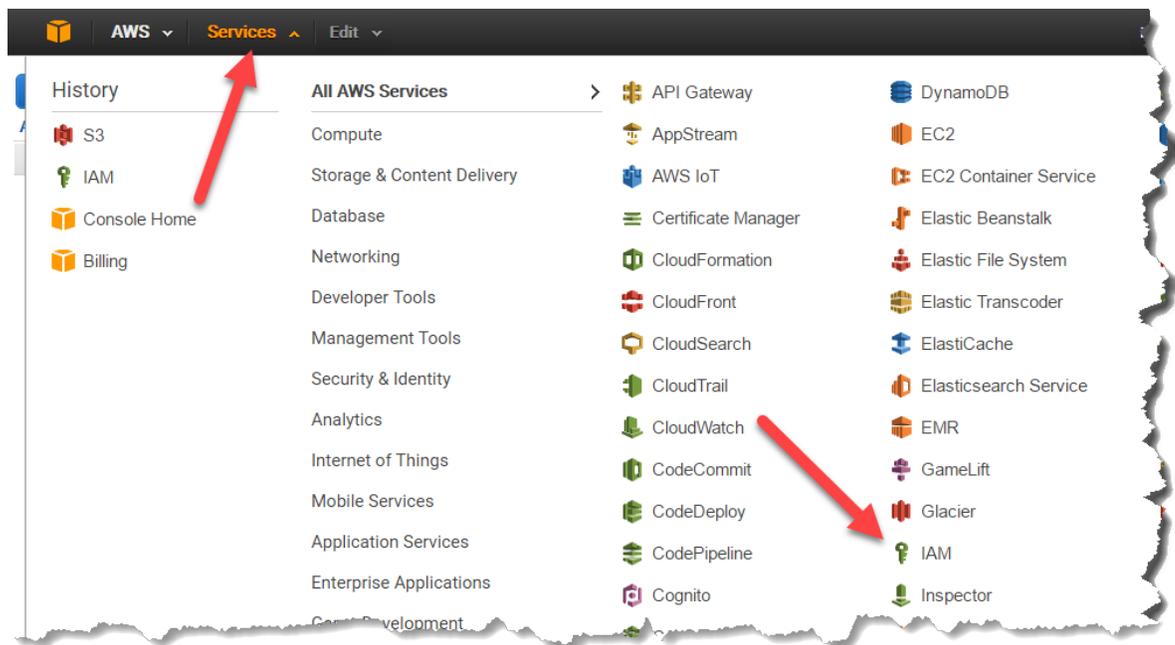


then

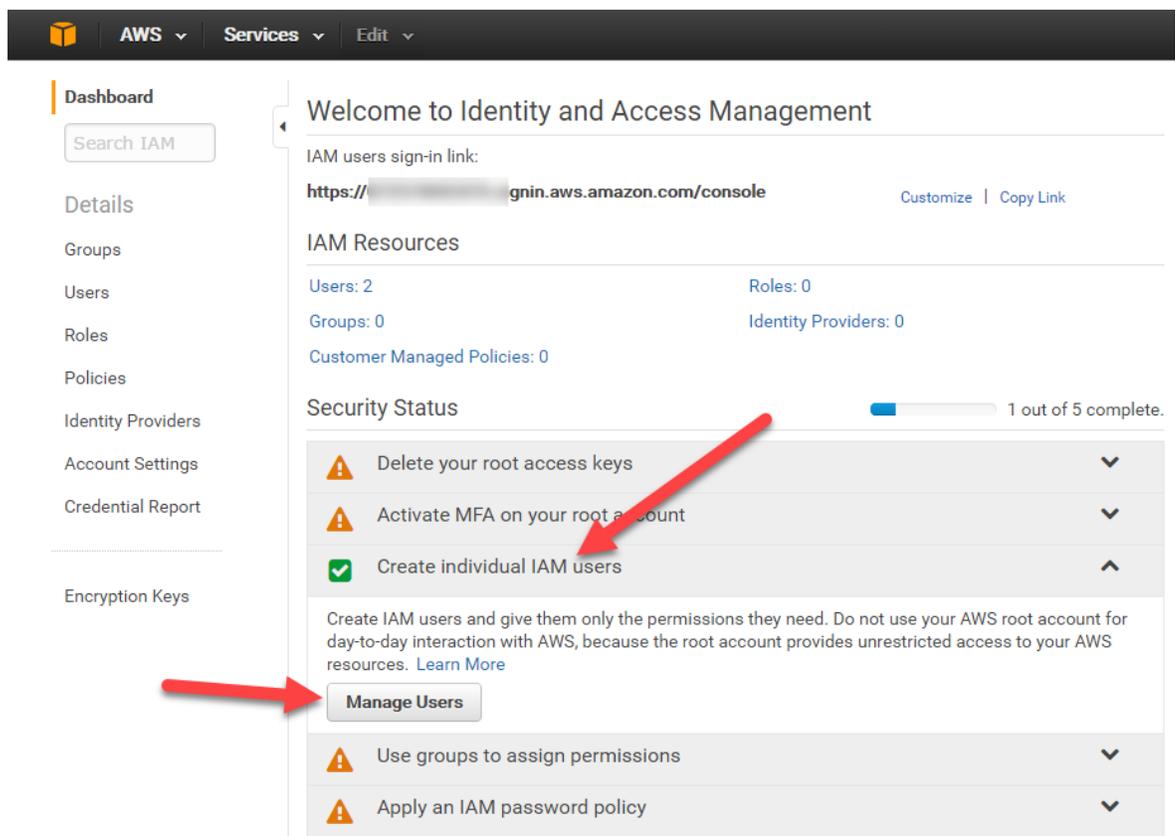


The Bucket name must be unique on the entire Amazon S3 system. Choose the most suitable region for your requirements, such as legal requirements for security & confidentiality of the data.

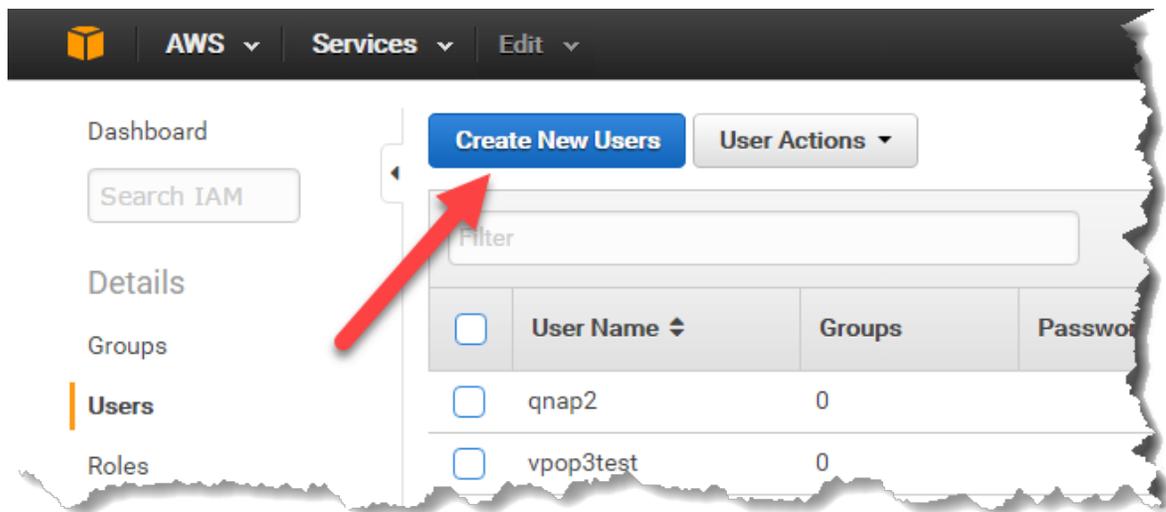
Now, you need to create security credentials for VPOP3 to access the bucket. Click on **Services** on the toolbar, then **IAM**.



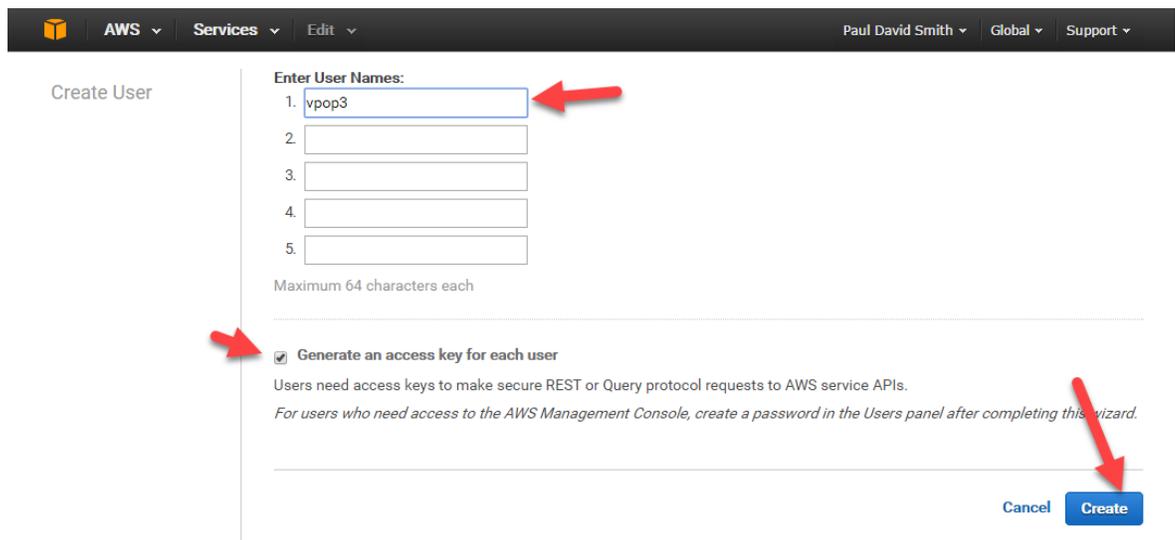
Select **Create Individual IAM Users** and **Manage Users**.



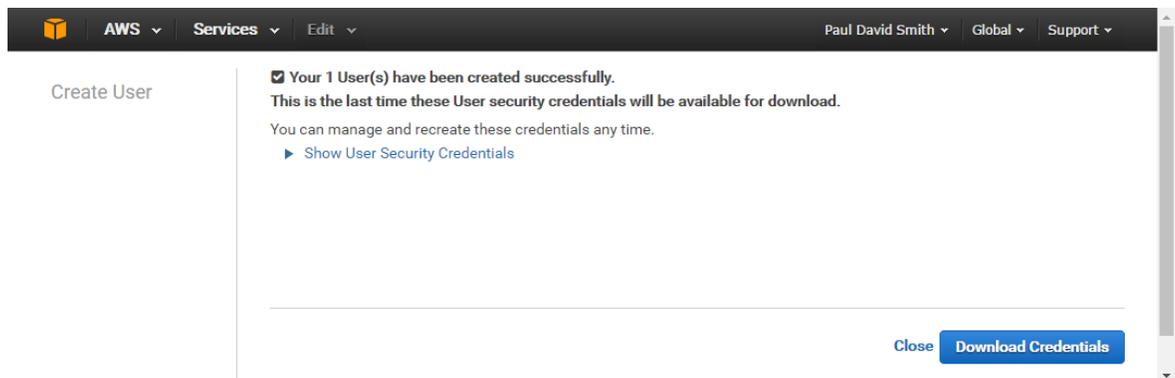
This will show you a list of current users (which may be blank). Choose **Create New Users**



Enter a new user name, eg 'vpop3' and check **Generate an access key for each user** and press **Create**.



Your user will be created



Press **Show User Security Credentials**

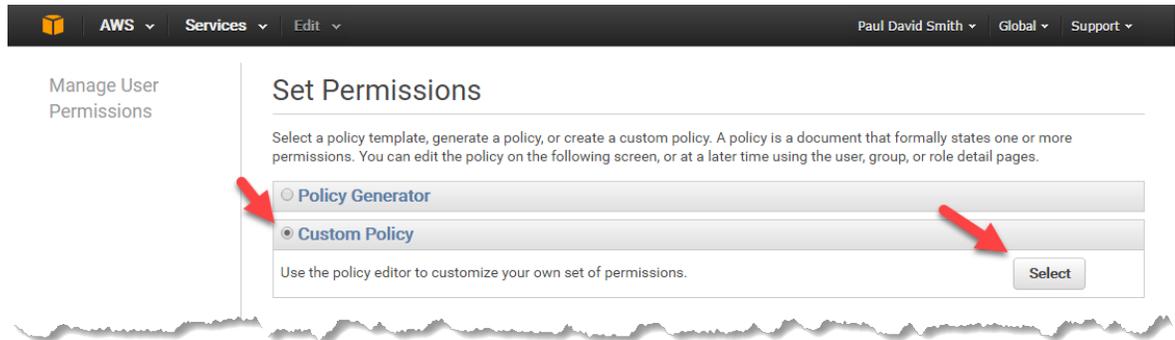
The screenshot shows the AWS IAM console notification for a user creation. At the top, it says "Your 1 User(s) have been created successfully." Below this, it states "This is the last time these User security credentials will be available for download." and "You can manage and recreate these credentials any time." There is a dropdown menu for "Hide User Security Credentials". The user details for 'vpop3' are shown in a yellow box: Access Key ID: AKIAJIYQFIFZ6DA4EFTQ and Secret Access Key: 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. At the bottom right, there are "Close" and "Download Credentials" buttons.

Take a note of these credentials. You can not recover the Secret key if you do not take note of it (you will need to create a new set of credentials in that case). You can also download them to your local PC for future reference.

After closing that window, you will be taken to your new list of users. Select the user you have just created, and go to the **Permissions** tab. You will see that there are no permissions for the new user. Expand the **Inline Policies** section and click to create a new inline policy.

The screenshot shows the AWS IAM console for user 'vpop3'. The 'Permissions' tab is selected. Under 'Managed Policies', it says "There are no managed policies attached to this user." with an "Attach Policy" button. Under 'Inline Policies', it says "There are no inline policies to show. To create one, [click here](#)." Two red arrows point to the "Attach Policy" button and the "click here" link respectively. The footer contains "Feedback", "English", "© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.", "Privacy Policy", and "Terms of Use".

Select **Custom Policy**, then **Select**



In the Policy Name, put something appropriate, such as 'VPOP3.Backup.Access'.

In the Policy Document, put something like:

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::vpop3backup",
        "arn:aws:s3:::vpop3backup/*"
      ]
    }
  ]
}
```

Replace "vpop3backup" with the name of the S3 Bucket you created earlier. Press **Apply Policy**

Once you have created the S3 Bucket Name and have the security credentials, enter the S3 Bucket name, Access key and Secret Key into the VPOP3 settings.

You can click the **Compress messages before uploading** button to have VPOP3 compress the messages (using GZIP) before uploading them).

If you set an **Encryption Key**, then VPOP3 will encrypt the messages with the supplied encryption key using the Blowfish algorithm before uploading them. Note that *the encryption key is not recoverable*, so if you set this, *do not lose it*.

If you change the Compression or Encryption options after enabling S3 backup, then VPOP3 will have to start the backup process from the beginning so that the messages are compressed/encrypted as appropriate.

When you press **Save Settings**, then the S3 and compression/encryption options will be saved in VPOP3.

You can then check **Upload messages...** or **Download messages...** depending on whether you want VPOP3 to backup or restore messages. While either of these options is checked, you cannot alter the S3 settings. You can enable both options to allow multi-master mirroring between two VPOP3 servers (assuming you have the appropriate licences) using the S3 store as an intermediary, but note that this is asynchronous mirroring so, while it is OK to do if different users usually use different servers, but if one user can use both servers at the same time, then they may encounter strange behaviour.

The **Upload status** and **Download status** sections show the upload & download status of the S3 backup facility.

See also: [Offsite Backup](#)

5.6.5.6 Restore

To get to this page, go to Settings → [Database](#) -> Restore (VPOP3 Enterprise Only).

The screenshot shows the VPOP3 Enterprise 6.20 web interface. The left sidebar contains a navigation menu with categories like Admin Settings, Anti-virus, Attachment Processing, Autoresponder Settings, Database, Diagnostics, FaxServer, Global Address Book, Global Signature, Groups, Header Processing, Receipts/Urgent Messages, Global Header Modifiers, Legacy Extensions, Listserver Settings, Local Mail, Logging, Message Archive, Message Authentication, Message Monitoring, Misc Settings, Plugins, Quotas, Scripts, Security Settings, SMS, Spam Filter, and VPOP3 Text Strings. The main content area is titled 'Database' and has a 'Submit' button. Below this is a tabbed interface with tabs for 'Message Store', 'Search Index', 'Amazon S3 Backup', 'Restore', and 'Offsite Backup'. The 'Restore' tab is active, showing the following configuration options:

Restore

This *Restore* facility is to restore individual users' mail folders if they have been deleted. (Also see the 'recycle bin' facility in the user's **Advanced** settings). For a full server restore, see the [support Wiki](#). To use this facility you must first restore the relevant database backup into a temporary database on a PostgreSQL server, and specify the connection details below.

(**Connection String** : `host=192.168.66.101 user=postgres password=pgsqlpass port`)

Server : 192.168.66.101

Username : postgres

Password : pgsqlpass

Port : 5433

Connection Status :

Database : vpop3_1

Name	Count	Size
<input type="checkbox"/> autoresp		
<input type="checkbox"/> @gauto		
<input type="checkbox"/> paul		

Target User: Original User (create if doesn't exist)

Target Folder:
(Leave blank for original folder)

Restored Message Flags: No Changes Mark Unread Mark Flagged

VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23 | Idle | In: 40379 | Out: 0

The Database Restore function lets you restore messages from a database backup without doing a full restore.

If messages have been deleted recently (typically within the last few days, depending on the [settings](#)), then you can use the [Message Recycle Bin](#) function to restore messages quickly and easily.

If you need to perform a full restore of VPOP3 to restore users, settings, etc then see the [Restoring a Backup](#) topic.

If the wanted messages were deleted too long ago to be recoverable from the Message Recycle Bin, but you only want to restore messages for specific user(s) or folder(s) then the Database Restore function is what you need.

■ Preparing for Database Restore

To use the Database Restore function, there must be a PostgreSQL database containing the backup you want to restore into your live VPOP3. This database be on the VPOP3 PC itself or on any other PC which this VPOP3 can connect to over a network. The main consideration will probably be available disk space. The entire backup will need to be restored into a temporary database, so whilst you are doing the restore process, it will use as much disk space as the full database. As a rule of thumb, this will be about twice the size of the database backup file.

Using a different computer for the temporary database

If you wish to use another computer, then you need to install PostgreSQL onto that other computer first. This can be downloaded from <https://www.postgresql.org/download/>. For this purpose, you can use any version of PostgreSQL from 9.1 upwards and it can run on any operating system supported by PostgreSQL.

Once you have installed PostgreSQL you need to edit two files so that VPOP3 can connect to it over the network.

Postgresql.conf

Edit the postgresql.conf file in the PostgreSQL data folder. Add a line saying:

```
listen_addresses='*'
```

pg_hba.conf

Edit the pg_hba.conf file in the PostgreSQL data folder. Add a line saying something like:

```
host all all 192.168.0.52/32 md5
```

(change the 192.168.0.52/32 as appropriate to indicate the IP address of the PC where your VPOP3 server is)

After making these changes, restart the PostgreSQL server on the other PC (not the VPOP3 PC). Also, make sure that any firewall software on this PC is configured to allow access to the PostgreSQL service (or disabled).

Restoring the temporary database

On the VPOP3 PC, or the temporary PostgreSQL PC, you now need to restore the VPOP3 backup you wish to restore messages from.

First, find the database backup. By default VPOP3 creates daily backups (cycled weekly) called DBBACK-x.TMP in the VPOP3 installation directory, but you may have changed these filenames or told VPOP3 to store them elsewhere.

Next, on the PC where you want to restore the temporary database, open a command prompt, and go to the PostgreSQL 'bin' directory,

eg, on a VPOP3 PC you may type:

```
cd c:\vpop3\pgsql\bin
createdb -p 5433 -U postgres -E SQL_ASCII vpop3temp
pg_restore -U postgres -p 5433 -v -d vpop3temp dbback-x.tmp
```

At password prompts, use 'pgsqlpass'

On a temporary PostgreSQL server PC, you may use something like:

```
cd c:\pgsql\bin
createdb -U postgres -E SQL_ASCII vpop3temp
pg_restore -U postgres -v -d vpop3temp dbback-x.tmp
```

At password prompts, use the password you created while installing PostgreSQL.

This restore process may take a while.

Once you have the database backup restored in a temporary database, you can tell VPOP3 to retrieve messages from it

In **Server**, put the IP address of the temporary database server (localhost if it is on the VPOP3 PC)

In **Username & Password**, put the PostgreSQL administrator username & password (default 'postgres' and 'pgsqlpass' if on the VPOP3 PC)

In **Port**, put the PostgreSQL service port (default 5433 if on the VPOP3 PC or 5432 if on a separate PC)

Now, the **Database** drop-down should be populated with the available databases. Choose the temporary database you created above - eg 'vpop3temp'

Once you have chosen that, the box at the bottom of the page should be populated with the users & folders available in that database. You can expand the trees to select folders. Select multiple users & folders by using shift-click and ctrl-click as normal.

Once you have chosen the users & folders to restore, you can choose the **Target User** which is the user where the messages will be restored to. You can tell VPOP3 to put the messages into the original user's mailbox, or a specified user's mailbox.

You can also choose the **Target Folder**. Leave this blank to use the original folder name. (If the folder exists, VPOP3 will add the restored messages into that folder. Existing messages will be left).

You can also tell the restore process to mark restored messages as unread, flagged (starred) or leave them with the status in the backup.

When you are ready press **Start Restore**. VPOP3 will now display a list of folders it is restoring and display the progress. Messages will appear in users' mailboxes as they are being restored.

5.6.5.7 Offsite Backup

To get to this page, go to Settings → [Database](#) -> Offsite Backup

The Offsite Backup settings let VPOP3 upload messages to our cloud backup service. VPOP3 uploads message and message status changes as they occur, and it only needs to upload changes, rather than being a full backup just once a day as the local backup facility is. However, the Offsite Backup is purely for messages. Users, Mappings and other settings are not backed up using this facility. The cloud backup server runs server software which knows about VPOP3 and can help with handling message status updates and restores - it is not a plain file store.

If/when the VPOP3 server fails, you can install VPOP3 on a new PC, and put in the same Offsite Backup Key and press the **Start Offsite Restore** button. The new server will then start restoring messages from the cloud service. It restores messages in reverse order - newest ones first, to make it possible to start working sooner than if it restored oldest messages first.

You can even run two VPOP3 servers at the same time (two licences will be needed) and have the main one backing up to the cloud service, and the second one running a restore service constantly, to keep up-to-date with the live system. This may be an alternative to replicating the VPOP3 database, especially if the two servers are in different locations, with the advantage of having an offsite copy of messages as well.

The Offsite Backup service is a chargeable service - see [VPOP3 Offsite Backup on our website](#) for more information, including prices.

Once you have signed up to the Offsite Backup service, we will send you an **Offsite Backup Key**, which you enter into the VPOP3 software and press **Save Key** to validate and store the key, then you press the **Start Offsite Backup** button to start backing up offsite. You can press the **Pause Backup** button to temporarily pause uploading data. The **Stop Offsite Backup** button can be used to totally stop the backup operation. If you then want to restart the backups, VPOP3 will have to start its upload from the beginning, so don't stop the backup as a temporary action.

To restore messages, enter the same Offsite Backup Key as you used for backing up the messages, and press the **Start Offsite Restore** button to start the restore operation.

The **Backup Status** will show how many messages are stored offsite and how many are queued to be uploaded. In the Queued Items, the first number is the number of message status indicators which need to be uploaded (read/unread, flagged, folder names etc) and the second number is the number of messages themselves which need to be uploaded. If a message is marked read, VPOP3 doesn't need to upload the message again, just an indicator to show that its status has changed.

The **Restore Status** will show the status of any restore operation, including whether it is running on this or another server, and how many messages & folders are waiting to be downloaded by that other server.

See also: [Amazon S3 Backup](#)

5.6.6 Diagnostics

The Diagnostics settings allows you to configure what diagnostic data is logged and how long it is kept as well as a diagnostic tool.

- [General Tab](#)
- [Session Logs Tab](#)
- [Temporary/Archived Files Tab](#)
- [Log File Sizes Tab](#)
- [Retention Tab](#)
- [Message Trace Tab](#)
- [Message Search Tab](#)
- [Log File Writer Tab](#)
- [SysLog Tab](#)

5.6.6.1 General

To get to this page, go to Settings → [Diagnostics](#) → General

The screenshot shows the 'Diagnostics' settings page for VPOP3. At the top, there is a 'Show Hints' button and a 'Submit' button. Below these are tabs for 'General', 'Session Logs', 'Temporary/Archived Files', 'Log File Sizes', and 'Message Trace'. The 'General' tab is selected, showing 'General Settings'. The settings include: 'Log Path' set to 'z:\logs', 'Log Level' set to 'Full Logging', and 'Maximum log size' set to '9998 kB'. There is a checked checkbox for 'Buffer logging data' with a note: '(Improves logging performance, requires restart on change)'. Below these are buttons for 'View Main VPOP3 diagnostics Log' and 'View Error Log'. A section titled 'View Other Log Files' contains buttons for 'View Security Log', 'View Connection Log', 'View Download Rules Log', 'View SMTP Rules Log', 'View MAIL.LOG', and 'View Virus Scanner Log'.

The **Log Path** setting tells VPOP3 where to store diagnostic log files. The default location is the **_logs** directory inside the main VPOP3 installation directory. It can improve performance on busy servers if you set the logging directory to be on a different disk from the main VPOP3 installation, especially if you have turned on lots of logging options. If you have the available RAM, then telling VPOP3 to log to a RAM-Disk is the best option, but we do not recommend logging to an SSD drive because the large amount of writing can greatly reduce the life of SSD drives. You can use [file path macros](#) in this setting.

The **Log Level** setting tells VPOP3 how much diagnostic data to log to the **VPOP3.LOG** file. There are 4 settings, going from **Errors Only**, **Level 1**, **Level 2** to **Full Logging**. The higher logging options can affect performance, so we recommend you leave it on **Errors Only** unless you are trying to diagnose a particular problem or Technical Support tells you to increase the log level.

The **Maximum log size** sets the maximum size of the **VPOP3.LOG** file. When the log file fills up, VPOP3 renames it to **VPOP3.LBK** (after deleting any existing **VPOP3.LBK** file) and starts a new **VPOP3.LOG** file. See the [Log File Sizes](#) and [Retention](#) tabs for more information.

The **Buffer logging data** option tells VPOP3 to buffer logging data in memory, and write it to disk in the background, using the [Log File Writer](#).

The remaining buttons on the page allow you to view the log files in your web browser. (They can also be viewed directly from the **Log Path** directory on the VPOP3 server. They are plain text files, so can be opened in any text editor that can handle the large files).

- **View Main VPOP3 Diagnostics Log** - this lets you view the **VPOP3.LOG** file, where VPOP3 stores its processing diagnostic entries. This contains information on decisions made by VPOP3, etc. The level of detail in this log file is adjusted by the **Log Level** setting above.
- **View Error Log** - this lets you view the **ERRORS.LOG** file. VPOP3 stores error information here. Note that although it is called the *Error Log* it may contain entries which may not represent errors from

VPOP3. For instance, it will contain entries for dropped connections, but that is because the remote computer has dropped the connection - VPOP3 couldn't do anything about it. These are logged in this file because it is not normal, so they may be useful when trying to diagnose problems encountered when sending messages from an email client, for instance.

- **View Security Log** - this lets you view the **SECURITY.LOG** file. VPOP3 logs failed login attempts (and [optionally](#), successful login attempts) in this file. This file contains more information about why a login failed than is returned in the error message to the user. The user is just given a generic 'login failed' type error message to avoid helping an attacker, but this log file will indicate whether it is a bad password, unknown username, permission problem, etc.
- **View Connection Log** - this lets you view the **CONNECT.LOG** file. This contains a summary of connection information, similar to that shown in the [VPOP3 Status view](#) or [Status Monitor](#).
- **View Download Rules Log** - this lets you view the **DLRULES.LOG** file. This contains actions taken by a [Mail Collector's Download Rules](#) when downloading messages from a remote POP3 server.
- **View SMTP Rules Log** - this lets you view the **SMTPRULES.LOG** file. This contains actions taken by an [SMTP Server's SMTP Rules](#) when accepting messages sent using SMTP.
- **View MAIL.LOG** - this lets you view the **MAIL.LOG** file which contains a summary of messages sent today. (At the end of each day, this file is renamed to **MAILLOG.MON**, **MAILLOG.TUE**, etc with the extension being the first 3 letters of the relevant day of week, in English. Hence, it cycles weekly).
- **View Virus Scanner Log** - this lets you view the **VIRUSCAN.LOG** file which contains a list of all message parts/attachments scanned, and the scan result (only if you are using the optional VPOP3 Antivirus plugin)

Please note that entries in any log files do not necessarily indicate a problem. We will not offer support just generally explaining what is in log files. The log files are meant to help diagnose a problem that you have noticed such as problems sending messages. They are not meant to be used to indicate that there is a problem in the first place.

5.6.6.2 Session Logs

To get to this page, go to Settings → [Diagnostics](#) → Session Logs

The screenshot shows the VPOP3 Admin Settings interface. The left sidebar contains a tree view of settings categories. The top toolbar includes icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. The main content area is titled 'Diagnostics' and has a 'Submit' button. Below the title is a tabbed interface with tabs for General, Session Logs, Temporary/Archived Files, Log File Sizes, Retention, Message Trace, and Message Search. The 'Session Logs' tab is selected. The page content includes a warning: 'Enabling session log files often causes a significant slowdown on the session type being logged. Only use these options if you are encountering a problem and/or have been advised to enable this logging by technical support.' Below this is a note: 'These logging options log ALL data sent between the two relevant servers, so will log a lot of data.' The 'Maximum log size' is set to 9997 kB. There is a text input for 'Only log this IP address'. The 'VPOP3 Service Logs' section has checkboxes for 'Log POP3 Server Connections', 'Log SMTP Servers' (with sub-options for New SMTP Server and SMTP Server), and 'Log IMAP4 Server Connections'. The 'VPOP3 Connector Logs' section has checkboxes for 'Log POP3 Collectors', 'Log Mail Senders', and 'Log NNTP Collectors'. Each checkbox has a 'View' button next to it. At the bottom of the page, there is a status bar showing 'VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23' and user status 'idle | In: 42300 | Out: 0'.

Session Logs record the full conversation between VPOP3 and other computers at the raw protocol level (without any session encryption). They can be used for trying to find why message sending or collection isn't working, but generally they will require some knowledge of the underlying Internet protocol, such as [SMTP](#), [POP3](#) or [IMAP4](#) as well as the Internet Message [format standards](#).

These log files can log a *lot* of data, especially if your server is busy, so you will probably need to consider setting the log file [Retention](#) settings as well otherwise the log may have been overwritten by the time you come to look at it. Enabling these log files will also slow things down. Generally we recommend they are turned off unless you have been asked to turn them on by one of our technical support representatives.

The **Maximum log size** setting tells VPOP3 how big to allow each log file to grow. This is the same for each log file on this page. When the log file fills up, VPOP3 renames it to ***.LBK** (after deleting any existing ***.LBK** file) and starts a new ***.LOG** file. See the [Log File Sizes](#) and [Retention](#) tabs for more information.

The **Only log this IP address** option lets you filter session logging by the remote computer's IP address which may be helpful if trying to diagnose a problem with a particular remote server or client. Enter the remote computer's IP address or subnet (use CIDR ranges if required - eg [192.168.1.0/24](#))

The **VPOP3 Service Logs** section configures logging for VPOP3 services - the parts of VPOP3 which provide services to email clients. This is usually where you need to log if there is a problem with the mail software on a user's computer or device. The SMTP service is also used for incoming SMTP messages.

If you just have one service defined of a particular type (always in VPOP3 Basic and by default in VPOP3 Enterprise), then you will just have one checkbox, as above for **Log POP3 Server Connections**. If you have multiple services defined (as above for SMTP), it will list the various services in the group with a checkbox for each.

The **VPOP3 Connection Logs** section defines logging for VPOP3 connectors - the parts of VPOP3 which communicate with remote mail servers. This is where outgoing SMTP mail is logged when being sent to a remote SMTP server and incoming POP3 from a remote POP3 server is logged. The various Mail Collectors and Senders you have defined can have logging turned on individually here.

The **View** buttons let you see the current log file of the particular type. The log files are also stored in the VPOP3 logging directory (defined on the [General](#) tab) as:

- **Log POP3 Server Connections - POP3SVR.LOG**
- **Log SMTP Servers Connections - SMTPSVR.LOG**
- **Log IMAP4 Server Connections - IMAPSVR.LOG**
- **Log NNTP Server Connections - NNTPSVR.LOG**
- **Log POP3 Collectors - POP3CLT.LOG**
- **Log Mail Senders - SMTPCLT.LOG**
- **Log NNTP Collectors - NNTPCLT.LOG**

Note that all connections of a particular type are logged in the same log file.

When the log file fills up, it is renamed to <whatever>.LBK, and a new .LOG file is created.

5.6.6.3 Temporary/Archived Files

To get to this page, go to Settings → [Diagnostics](#) → Temporary/Archived Files

The screenshot shows the VPOP3 Admin Settings interface. The top navigation bar includes links for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, and WebMail. The left sidebar lists various settings categories, with 'Diagnostics' selected. The main content area is titled 'Diagnostics' and has a green header indicating 'Changes have been applied'. Below this is a tabbed interface with 'Temporary/Archived Files' selected. The page content includes a section titled 'Temporary & Archived Error files' with a descriptive paragraph and three checkboxes: 'Keep Temporary Files', 'Automatically delete Temporary Files after 4 days', and 'Archive Error Files'. There are also buttons for 'Delete All Temporary Files Now' and 'Delete All Archive Files Now'. The status bar at the bottom shows 'VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23' and 'Idle | In: 44636 | Out: 0'.

This page allows you to enable a specific kind of logging, that is rarely (but occasionally) applicable in recent versions of VPOP3.

Because the files are now of very limited use, we do not recommend enabling these options, unless our Support team have specifically told you to do so.

When these settings are enabled, VPOP3 will rename certain redundant files, instead of deleting them, so they can be inspected afterwards.

There are three checkboxes:

- **Keep Temporary Files** (Rename files to D*.DAT to A*.DAT instead of deleting them)
- **Automatically delete Temporary Files after [-] days** - sets a maximum time for retaining old files, to limit the storage of old data
- **Archive Error Files** - retain files that may contain important diagnostic information, related to an error

There are two buttons, which will remove all retained temporary and error files:

- **Delete All Temporary Files Now**
- **Delete All Archive Files Now**

5.6.6.4 Log File Sizes

To get to this page, go to Settings → [Diagnostics](#) → Log File Sizes

The screenshot shows the VPOP3 Enterprise 6.20 web interface. The left sidebar contains a tree view of settings categories, with 'Diagnostics' selected. The main content area is titled 'Diagnostics' and has a 'Log File Sizes' tab selected. Below the tab, there is a list of log files with their current sizes and maximum allowed sizes in kilobytes (kB). The list includes:

Log File Name	Current Size	Maximum Size	File Name
Main Log File	9998	kB	(VPOP3.LOG)
Main Error Log File	1025	kB	(ERRORS.LOG)
Session Log Files	9997	kB	(SMTPSVR.LOG, POP3CLT.LOG etc)
Download Rules Log	1001	kB	(DLRULES.LOG)
SMTP Rules Log	1002	kB	(SMTPRULES.LOG)
Security Log	1003	kB	(SECURITY.LOG)
Virus Scanner Log	1004	kB	(VIRUSCAN.LOG)
External Router Log	100	kB	(EXTROUTER.LOG)
HTTP Client Log	100	kB	(HTTPLOG.TXT)
AV Update Log	100	kB	(AVUPDATE.LOG)
SMTP Transcript Log	100	kB	(SMTPTRANSCRIPT.LOG)
POP3 Transcript Log	100	kB	(POP3TRANSCRIPT.LOG)
Lua Errors Log	100	kB	(LUAERRORS.LOG)
Instant Messaging Log	1024	kB	(VPOP3_IM.LOG)
Spam Rules Log	1024	kB	(SPAMRULES.LOG)
WebMail Access Log	100	kB	(WEBMAIL.LOG)

When a log file reaches its maximum size, VPOP3 will rename the *.LOG file to *.LBK. If you have VPOP3 keeping more than one old log file (see the Retention tab), it will rename any existing *.LBK file to keep those as appropriate as well

VPOP3 Enterprise 6.20 - Imail.pscs.co.uk - 192.168.66.23 | Idle | In: 42432 | Out: 2

This page lets you set the maximum log file sizes in one place for the various log files which VPOP3 makes.

The file sizes will not be exact. The technical details below may help if you are interested.

Technical details on log file sizes & retention

When VPOP3 creates a log file, it creates an empty file of the appropriate size and keeps track of how far through the file it has written. This is to try to avoid excessive disk fragmentation which can happen if several files are appended to in an interleaved manner. When VPOP3 creates, say, a 10MB file, Windows will try to place it in a single contiguous block on the disk, which won't happen if the file starts off with zero length and then grows gradually. This means that if you view a log file directly, it will probably have lots of empty space at the end because that part of the file hasn't been written to yet.

When VPOP3 has written data to a log file which takes it over the maximum size for that log file, VPOP3 will rename the current file to <something>.LBK and create a new <something>.LOG file of the appropriate size. If there was already an LBK file, that will be deleted (unless **Retention** rules say otherwise). This means that you will always have the current log file (which may contain between zero and <max> bytes of log) and the previous log file which will contain at least <max> bytes.

If you want to store more logs, then the [Retention](#) tab lets you set log file retention rules. In that case, you can tell VPOP3 to keep log files for a certain amount of time, or a certain number of log files. In this case, rather than deleting old LBK log files, VPOP3 will rename the LBK file being replaced to

<something>_<date>_<number>.LBK. The <date> will be the date when the LBK file was renamed and the <number> will be a sequential number for the log files on that date. You can use the last-modified timestamp on the files to see what times' log entries are recorded in which files.

The retention rules will also tell VPOP3 how much disk space can be used by these log files and how much free space there must be left after creating the log files. In this case, VPOP3 will delete the oldest retained LBK file to meet the disk space requirements. (It will not delete the <something>.LBK log file, just any extra files it has kept).

5.6.6.5 Retention

To get to this page, go to Settings → [Diagnostics](#) → Retention

The screenshot shows the 'Log File Retention' settings page in the VPOP3 Admin Settings interface. The page is titled 'Diagnostics' and has a 'Submit' button. The 'Retention' tab is selected, showing settings for 'Log File Retention'. Under 'How long to keep OLD log files', there are two radio buttons: 'Keep 1 old log files' (selected) and 'Keep old log files for 3 days'. Under 'OLD Log file disk usage', there are two settings: 'Use no more than 3800 MB for old log files (*.LBK)' and 'Delete old log files (*.LBK) if less than 500 MB free disk space'. A paragraph explains that when a log file reaches its maximum size, VPOP3 will rename it to *.LBK and delete any old *.LBK files to meet its settings. A note states that VPOP3 will not delete any <logfile>.LBK files to meet its settings, just <logfile>_date_number.LBK files.

This page lets you set how long VPOP3 will keep log files that it generates.

By default VPOP3 will have the current log file and the previous version of the log file (saved as <something>.LBK), but often this doesn't allow you to look far enough back in time, so you can tell VPOP3 to keep more log files (obviously that will use more disk space)

The **How long to keep OLD log files** settings tell VPOP3 either how many old log files to keep or how long to keep old log files (in days).

The **OLD Log file disk usage** settings tell VPOP3 how to manage disk space used by the old log files. Note that these settings take precedence over the **How long to keep OLD log files** settings.

You can tell VPOP3 the maximum amount of disk space to use for the old LBK log files. You can also tell it how much free disk space there must be remaining for it to keep old log files.

VPOP3 processes these settings in a sensible order to prevent disk space being used up by the log files.

For instance, if you have told VPOP3 to keep log files for 3 days, and to use no more than 5000MB for the log files and to delete old log files if there is less than 10000 MB free disk space, then when VPOP3 needs to make a new LBK file, it will check all the usage and free space. It will process it as below:

- if there is < 10000MB of free space, then VPOP3 will delete the oldest extra LBK files to make the free disk space to at least 10000MB - regardless of how old they are and how much space they are taking up.
- if the LBK files take up more than 5000MB, then VPOP3 will delete the oldest extra LBK files to ensure that they use no more than 5000MB - regardless of how old they are.
- it will keep the oldest LBK files if there is at least 10000MB free, the LBK files take up no more than 5000MB and they are no older than 3 days.

For some more technical details see the [Log File Sizes tab instructions](#).

5.6.6.6 Message Trace

To get to this page, go to Settings → [Diagnostics](#) → Message Trace

The screenshot shows the VPOP3 Enterprise 6.20 Admin Settings interface. The left sidebar contains a tree view of settings categories, with 'Diagnostics' selected. The main content area is titled 'Diagnostics' and includes a 'Message Tracing' section. This section has search fields for 'Search Subject', 'Search From', and 'Search Any', along with a 'Search' button and a note that '(Most recent 100 matching messages will be listed)'. Below the search fields is a table of message traces:

Date	Subject	From
2016-07-06 15:53:2	Delivery Status (Message Send Error)	"Mail System" <Mailer_Daemon@buildhelp.pscs.co.uk>
2016-07-06 15:50:0	Delivery Status (Message Send Error)	"Mail System" <Mailer_Daemon@buildhelp.pscs.co.uk>
2016-07-06 15:49:5	Delivery Status (Message Send Error)	"Mail System" <Mailer_Daemon@buildhelp.pscs.co.uk>
2016-07-06 15:46:3	Delivery Status (Message Send Error)	"Mail System" <Mailer_Daemon@buildhelp.pscs.co.uk>
2016-07-06 15:44:0	Delivery Status (Message Send Error)	"Mail System" <Mailer_Daemon@buildhelp.pscs.co.uk>

Below the table is a 'Details' section with two subsections:

Message Information

- Client: 192.168.66.29
- From: "Mail System" <Mailer_Daemon@buildhelp.pscs.co.uk>
- Recipients: sales@pscscs.co.uk
- ReturnPath:
- Server: 192.168.66.70:25
- Service: SMTP Server
- Subject: Delivery Status (Message Send Error)
- Type: SMTP

Trace Information

- 2016-07-06 15:49:47: MAIL FROM:<>
- 2016-07-06 15:49:47: RCPT TO:<sales@pscscs.co.uk>
- 2016-07-06 15:49:53: CheckMappings - sales@pscscs.co.uk - -1 - 1 - 0 - 0
- 2016-07-06 15:49:53: Found Mapping to sales
- 2016-07-06 15:49:53: Add Recipient sales
- 2016-07-06 15:49:53: Expand Recipient sales
- 2016-07-06 15:49:53: Distribute message
- 2016-07-06 15:49:53: Distribute message to sales
- 2016-07-06 15:49:53: Distribute message to mail folder(s)
- 2016-07-06 15:49:53: Stored in sales:Inbox (5047901 UID 73800224)

At the bottom of the interface, the status bar shows: VPOP3 Enterprise 6.20 - Imlmail.pscscs.co.uk - 192.168.66.23 | Idle | In: 42351 | Out: 0

This page lets you see how VPOP3 has processed recent messages. If you know VPOP3 should have received a message but it has not been delivered, or has been delivered incorrectly, you can search for it on this page, and VPOP3 will display key trace information to help diagnose what went wrong.

First, you should enter as much detail as you can into the **Search Subject**, **Search From** and **Search Any** fields. The **Search Any** searches any of the traced message's information fields, such as sender IP address, recipients, etc - see below.

Then, press **Search** to see a list of the most recent 100 messages which match the search data. VPOP3 keeps this data for 1 week, so there may be fewer than 100 matching messages.

Select the message you wish to investigate in the list of found messages.

VPOP3 will now display data in the **Details** section below the list of messages. There are two parts to this information:

- **Message Information** - this contains details about the message to help identify it. The data here will depend on how the message arrived at VPOP3 (SMTP or POP3) and other details such as authenticated senders, and so on. This data is unordered and just helps to identify the message.
- **Trace Information** - this contains an ordered list of key events in the processing the message. For example in the above screenshot this shows that the message arrived at VPOP3 using SMTP, and the SMTP 'RCPT TO' command indicated 'sales@pscs.co.uk' as the recipient. VPOP3 found a Mapping of sales@pscs.co.uk -> sales, so it added that recipient to the message, and eventually delivered the message to 'sales', storing it in the sales 'Inbox' folder, with an internal message ID of 5047901, and a UID of 73800224.

The information displayed may be a bit technical, but reading it will often help to highlight what happened, such as an unexpected Mapping causing misdelivery of the message, or that the message was quarantined, etc.

5.6.6.7 Message Search

To get to this page, go to Settings → [Diagnostics](#) → Message Search (this page is only present in VPOP3 Enterprise)

The screenshot shows the VPOP3 Admin Settings interface. The left sidebar contains various configuration categories such as Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, and Search. The main content area is titled 'Diagnostics' and features a 'Message Search' section. This section includes a 'Submit' button and a 'Search' button. Below the search filters, a table displays the search results. The table has columns for Date, Subject, and From. The first row is highlighted, showing a message from 'no-reply@kickstarter.com' with the subject 'Project Update #15: Nerdy Inventions - The Crazy Inventions Dice Game by Seth Hiatt'.

Message Search

This facility will search for messages in the message store and show you which user/folder they are in and if they have been recently deleted.

Search Subject :

Search From :

Search Message Content :

Search Attachment Name :

Date	Subject	From
2016-07-07 04:12:3	Project Update #15: Nerdy Inventions - The Crazy Inventions Dice Game by Seth Hiatt	no-reply@kickstarter.com
2016-07-07 04:12:3	Project Update #15: Nerdy Inventions - The Crazy Inventions Dice Game by Seth Hiatt	no-reply@kickstarter.com
2016-07-07 00:53:3	Project Update #25: Twist Of Fate - The Oliver Twist microgame for 2-4 players	no-reply@kickstarter.com
2016-07-07 00:53:3	Project Update #25: Twist Of Fate - The Oliver Twist microgame for 2-4 players	no-reply@kickstarter.com
2016-07-06 19:45:2	Project Update #7: Continental Divide: Railroads, Trains, Stock, Barons & Guts!	no-reply@kickstarter.com
2016-07-06 19:45:2	Project Update #7: Continental Divide: Railroads, Trains, Stock, Barons & Guts!	no-reply@kickstarter.com

<< 1 to 100 >>

Details

Message Information

- subject: Project Update #15: Nerdy Inventions - The Crazy Inventions Dice Game by Seth Hiatt
- fromaddr: no-reply@kickstarter.com
- folder: Inbox
- username: paul
- messagetime: 2016-07-07 05:12:36+01
- internaltime: 2016-07-07 05:07:25.258+01
- tolist: paul@psecs.co.uk
- deletedtime: 2016-07-07 09:06:49.667+01
- deletedreason: IMAP4-paul-192.168.66.101
- deleted: f
- hold: f
- size: 62832
- updatetime: 2016-07-07 09:06:49.667+01

VPOP3 Enterprise 6.20 - Imail.psecs.co.uk - 192.168.66.23 | Idle | In: 42629 | Out: 2

This page lets you search the VPOP3 message store for a message. Enter the search data in the boxes at the top of the page and press **Search**. To search on message content or attachments you need to have enabled the Full Text Search facility. See our [knowledgebase](#) for details of how to set this up.

Once you have pressed search, then a list of all the messages which match the search criteria will be displayed. This will show messages present in the message store, as well as messages in the [Message Recycle Bin](#) (if enabled).

If you select a message in the list, VPOP3 will display information about that message in the **Message Information** section below the list. Some of the information displayed is described below:

- **username** - this is the VPOP3 user in whose mailbox the message is stored.
- **folder** - this is the folder name where the message is stored
- **messagetime** - this is the date/time from the message's 'Date' header

- **internaltime** - this is the date/time the message was stored in VPOP3's message store
- **deletedtime** - this is the date/time the message was deleted from the VPOP3 message store (if the message is still in the Message Recycle Bin)
- **deletedreason** - this is text indicating why the message was deleted from the VPOP3 message store (eg in the screenshot above, it was deleted using IMAP4 by user 'paul' from IP address 192.168.66.101)
- **deleted** - this is the IMAP4 'deleted' flag (note that, as above, this may be f(false) even though the message has been deleted and vice versa. Messages are marked as deleted by IMAP4 clients, but still exist, then when the IMAP4 client purges (expunges/compacts) the folder, the message is *actually* deleted.
- **hold** - this is the VPOP3 'hold' flag for the message. A held message is invisible to email clients. The administrator can unhold the message in the [user's message list](#) in the settings.
- **updatetime** - this is when the message details/flags were last modified.

5.6.6.8 Log File Writer

To get to this page, go to Settings → [Diagnostics](#) → Log File Writer

The screenshot shows the VPOP3 Enterprise 6.20 web interface. The left sidebar contains a navigation menu with categories like Admin Settings, Anti-virus, Attachment Processing, etc. The main content area is titled 'Diagnostics' and has a 'Log File Writer' tab selected. The settings for the Log File Writer are as follows:

- Enable logging to file (not recommended to turn off!)
- Min Time between log writer bursts: 0 ms
- Max Time between log writer bursts: 10000 ms
- If lines written < 500 then increase time between bursts by 10 ms
- If lines written > 1000 then decrease time between bursts by 100 ms
- Only write to disk if at least: 10 lines waiting to be written
- Always write if oldest line is over: 10000 ms old
- Current time between log writer bursts: 310 ms

Below the settings is a 'Log file stats' section with a dropdown for 'Show stats for the last 1 hour'. A table displays the following data:

Name	Writes	Total Lines	Average Lines/Write	Average Lines/sec	Total Bytes	Average Bytes/Write	Average Bytes/sec
ssobackup.log	0	0	0	0	0	0	0
security.log	21	51	2.42	0.21	4.4kB	214	19
smtpdlt.log	0	0	0	0	0	0	0
smtprules.log	18	149	8.27	0.64	24.8kB	1.4kB	109
smtpsvr.log	222	18234	82.13	78.19	1.7MB	7.9kB	7.5kB
smtpsvrtranscript.log	128	2560	20	10.97	127.9kB	1023	561
smtptranscript.log	0	0	0	0	0	0	0
spamrules.log	171	3770	22.04	16.16	425.5kB	2.5kB	1.8kB
viruscan.log	0	0	0	0	0	0	0
vpop3.log	926	246908	266.63	1046.92	28.9MB	32kB	125.5kB
vpop3_im.log	0	0	0	0	0	0	0

At the bottom of the page, the status bar shows: VPOP3 Enterprise 6.20 - Iml.pscs.co.uk - 192.168.66.23 | Idle | In: 42708 | Out: 1

This page lets you configure and monitor the log file writer.

If **Buffer logging data** is enabled on the [General](#) tab, then whenever VPOP3 wants to write data to a log file, it does not write it directly. Instead it stores it in memory and a background process (the log file writer) writes the data to disk in chunks. This helps performance because it reduces disk activity.

The **Enable logging to file** option should be turned on. If this is turned off, then the log file writer will simply discard log entries, and they will never be written to disk! In general, it is better to disable specific logging options on the **General** and **Session Logs** tabs instead.

The next section configures how often the background writer will write a chunk of log data to disk. The longer between writes the less disk load there will be, but the more chance that a crash will cause log data to be lost and the more RAM will be used by the buffered data. VPOP3 has an internal counter which is the time between write bursts. The current value of this is displayed as **Current time between log writer bursts**. VPOP3 adjusts this time based on activity.

- **Min time between log writer bursts** - this sets the lowest value for the time between write bursts.
- **Max time between log writer bursts** - this sets the highest value for the time between write bursts
- **If lines written < X then increase time between bursts by Y ms** - if there are fewer than X lines to be written when the log writer performs a write action, then the time to the next write action will be increased by Y milliseconds. This means that if activity lessens, VPOP3 will wait longer between write bursts. The time will never increase to more than the **Max time between log writer bursts** value.
- **If lines written > X then decrease time between bursts by Y ms** - if there are more than X lines to be written when the log writer performs a write action, then the time to the next write action will be decreased by Y milliseconds. This means that if activity increases, VPOP3 will wait less time between write bursts. The time will never decrease to less than the **Min time between log writer bursts** value.
- **Only write to disk if at least X lines waiting to be written** - If there are fewer than X lines waiting to be written to a log file, then the log file writer will skip writing to that log file for now.
- **Always write if oldest line is over Y ms old** - even if there are too few lines waiting (as defined above), then the log file writer will still write them to disk if they are older than this. This prevents log files which only occasionally get new entries from never being written to disk.

Below this is the **Log file stats**. This section shows you how often each log file is written to. This can help with diagnosing issues with heavy disk load in some cases. For instance, in the above screenshot you can see that the VPOP3.LOG is heavily used, with 125kB being written each second to that file. This is because we have enabled **Full Logging** in the diagnostics General tab, so VPOP3 is writing a detailed log file. If we had disk performance issues it would help to reduce the log level to reduce the amount of data being written. (In our case this isn't necessary because VPOP3 is writing logs to a RAM disk whose performance is extremely quick).

5.6.6.9 SysLog

To get to this page, go to Settings → [Diagnostics](#) → Syslog (this page is only present in VPOP3 Enterprise)

SysLog

VPOP3 can send log entries to a SysLog server instead of to log files

Syslog Server :
(IP address, not host name - empty=disabled, 0.0.0.0=discard log entries)

Syslog Server Port :
(Default 514)

dirrules.log	<input type="button" value="Log to File"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="5"/>
httpclient.log	<input type="button" value="Log to File"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="7"/>
pop3svrtranscript.log	<input type="button" value="Log to File"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="6"/>
pop3transcript.log	<input type="button" value="Log to File"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="6"/>
security.log	<input type="button" value="Log to File"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="46"/>
smtprules.log	<input type="button" value="Log to File"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="5"/>
smtpsvrtranscript.log	<input type="button" value="Log to File"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="6"/>
smtptranscript.log	<input type="button" value="Log to File"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="6"/>
spamrules.log	<input type="button" value="Log to File"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="7"/>
viruscan.log	<input type="button" value="Log to File"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="46"/>
vpop3.log	<input type="button" value="Both"/>	Facility: <input type="text" value="Mail"/>	Severities: <input type="text" value="23567"/>

[Syslog](#) is a standard for message logging. It is more widely known in Linux systems, but there are Windows Syslog servers. Syslog lets you centralise logging for several services in one place, and there are tools which will monitor Syslog logs and perform automated actions.

On this page, you can tell VPOP3 the IP address for a Syslog Server in the **Syslog Server** and **Syslog Server Port** boxes. VPOP3 can then send Syslog messages to that server as configured below.

For each listed log file, VPOP3 can either **Log to File**, send to the **Syslog** server, or **Both** log to file and send to the Syslog server.

A Syslog message has several components - the **Facility**, **Severity** and **Message** itself. Other parts of the message are added automatically by VPOP3 (timestamp etc).

You can configure the **Facility** and **Severity** of the messages as you wish.

The default **Facility** is **Mail**, but you can choose other facilities as you require if it helps your Syslog server with monitoring or routing messages.

The various Syslog **Severity** values are:

0. Emergency
1. Alert
2. Critical
3. Error
4. Warning

5. Notice
6. Informational
7. Debug

Most log files have a single severity you can choose (the defaults are in the screenshot), but some have more than one:

- **security.log** - the first severity is used if a login failure is being logged; otherwise the second is used
- **viruscan.log** - the first severity is used if a virus is detected, otherwise the second is used
- **vpop3.log** - the various severities are used depending on the 'level' of the log entry (the first for critical errors, second for 'normal' errors, third for 'log level 1' and so on).

5.6.7 Global Signature

The **Global Signature** page lets you let "signatures" to be added to the bottom of messages. These can include company contact information, etc. (Note that disclaimers here are not necessarily legally significant, so we recommend consulting a lawyer before relying on them to mean anything).

VPOP3 Enterprise 6.15 - lmail.pscs.co.uk - 192.168.66.70

There are 4 tabs in the **Global Signature** page, but as all the tabs are very similar, we will describe them all below, rather than in separate sections.

The 4 tabs are:

- **Default Outgoing Signature** - the signatures here are added to the bottom of *outgoing* messages. This signature is used if the sender did not use SMTP authentication, or if the **Authenticated Users Outgoing** signatures are blank.
- **Authenticated Users Outgoing** - the signatures here are added to the bottom of *outgoing* messages sent by authenticated senders.
- **Default Internal Signature** - the signature here are added to the bottom of *internal* messages. This signature is used if the sender did not use SMTP authentication, or if the **Authenticated Users Internal** signatures are blank.
- **Authenticated Users Internal** - the signatures here are added to the bottom of *internal* messages sent by authenticated senders.

Outgoing vs Internal signatures

The signatures for internal and outgoing messages can be configured separately because most people do not require internal signatures or the signatures need to be quite different for internal use. This is because outgoing signatures often contain contact information, and legally mandated information such as company registration numbers, VAT numbers etc. For internal use, this information is redundant and unnecessary.

Authenticated Users vs Default signatures

The **Default** signatures can only contain fixed text or HTML which is the same for all senders.

Authenticated Users signatures can also contain data from the address book entries for the authenticated users (eg full name, direct-dial telephone number, etc). To indicate this in the signature use the format [**ldap attribute**], so, for instance, to include the 'common name' for the authenticated user you could use **[cn]**.

VPOP3 uses the *inetOrgPerson* objectclass for users, so you can use attributes defined in that object class. Some of the more useful ones are below:

- **cn** - common name/display name
- **gn** - first name
- **sn** - surname
- **mail** - email address
- **mobile** - mobile telephone number
- **title** - job title
- **ou** - department
- **physicalDeliveryOfficeName** - office
- **o** - company
- **postalAddress**, **l**, **st**, **postalcode**, **c** - postal address, city, state, post code, country
- **facsimileTelephoneNumber** - fax number

Plain text vs HTML signatures

You can define plain text and/or HTML signatures for each type of signature. VPOP3 will use the appropriate type of signature for the message you send. If you only provide one format of signature, VPOP3 will convert that signature to the other format as necessary. So, if you specify an HTML

signature, but send a plain text message, VPOP3 will strip HTML tags etc and create a plain text signature. It is often better to create both signatures manually so you can be sure the formatting is as you wish, but the automatic conversion can be useful.

It is important to know when the different signatures will be used. If you send a plain text message, and only have an HTML signature, VPOP3 will not convert the plain text message to HTML and attach the HTML signature. Instead it will convert the HTML signature to plain text and add that.

What format of message is sent does depend on the email client you are using, and its settings. For instance, with Mozilla Thunderbird, if you just send a simple message, without any formatting, it will send only a plain text message. If you include formatting (such as colours, bold text, different fonts, etc), then it will send the message as HTML, *and it will send an alternative plain text version of your message as well*. The recipient (or recipient's software) will choose which version of the message to display. For instance, if it is being imported into other software automatically, often the plain text version will be used, or if someone is reading the message in a text-only viewer (eg Pine on Linux) it will use the plain text version.

Note that if you use **Microsoft Rich Text** format when sending from Outlook, it will send the message as HTML, plain text AND Microsoft Rich Text format. VPOP3 can add signatures to the HTML and plain text versions of the message, but cannot add a signature to the Microsoft Rich Text version. If the recipient views the message in Outlook, they will probably see the Microsoft Rich Text version of the message, but if they view the message in anything else they will see the HTML or plain text versions.

Images in signatures

If you insert an image in an HTML signature, VPOP3 will **not** embed the image into the message. This is for several reasons - for instance, it can increase the size of your messages significantly, which will be inconvenient to people reading your message on mobile devices or metered connections, and it will usually require VPOP3 to totally rewrite the original message structure, which risks introducing bugs and unwanted behaviour.

Instead, the image in the signature will link to a URL which should point to an image on your website. So, if you want to show your company logo, you should insert an image with a link like <http://www.ourcompany.com/images/logo.png> (obviously the exact link will depend on where you have stored the image on your site). When the image is a link, then mobile users will often be asked whether they want to download the images, so they have the option not to use their bandwidth allowance.

Make sure the image you link to is the correct size. If you link to an image that is 1000x1000 pixels and you size it to 30x30 pixels in the HTML, then the email client still has to download the full 1000x1000 pixel image and rescale it at the user's end. If you link to a 30x30 pixel image, then the email client only has to download the smaller image which will be quicker and not use as much of the recipient's bandwidth allowance.

Generally, it's more considerate not to include images in your email signatures at all unless they are legally mandated, because the recipients will really not want to see them, and they just make your messages bigger and slower unnecessarily. If you force the recipient to use up their bandwidth allowance, they will be unhappy with you.

Personal Signatures

As well as the global signatures, users can have personal signatures defined in the **Edit User -> Outgoing Sig/Internal Sig** pages. You can also disable the global signature for users on those pages.

Which signature is used

If the sender does not authenticate, then the **Default Outgoing/Internal Signature** will be used.

If the sender does authenticate, then VPOP3 will look for a signature in the following order

1. If a Personal signature exists, VPOP3 will use that
2. If an Authenticated User signature exists, VPOP3 will use that
3. If a Default signature exists, VPOP3 will use that

VPOP3 detects whether a signature exists or not based on whether there is any content. So, if you actually want a Default signature to exist, but not to use a signature for authenticated senders, you cannot just leave the Authenticated User signature blank, because VPOP3 will fall back to using the Default signature. Instead, you need to specify the Authenticated User signature as "<blank>" (without the quotes). That text tells VPOP3 that that signature exists, but is to be blank.

Also, you can mix the Personal and Authenticated/Global signatures. If you include the text <personalsig> in the authenticated/global signature, VPOP3 will include the user's personal signature at that point. If you don't do that, and include the text <globalsig> in the personal signature, VPOP3 will include the personal signature at that point. (If you use both, then the <personalsig> tag takes precedence, it will not recurse indefinitely).

VPOP3 will remove any <personalsig> or <globalsig> tags which did not take effect, after it has finished expanding it, so you will not be left with those in the actual signature which is used.

You can also generate signatures dynamically using some [Lua scripting](#).

5.6.8 Groups

To get to this page, go to Settings → Groups

Name	Enabled	User Count	Force	In Everyone List	Allow Sending Internet Mail	Allow Receiving Internet Mail	Monitor	Admin	Max Outgoing Size (kB)	Reply Address
office	<input checked="" type="checkbox"/>	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0	
sasdadadsda	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	email@domain

If this is checked, all users in this group are forced to have the group's configuration. If this is not checked, new users in this group are given the group's configuration, but the users can then be changed individually

VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23 | Idle | In: 44812 | Out 1

In VPOP3, a Group is a sort of **List** which is also used for assigning permissions and settings. It can be used as a basic distribution list, but that use is secondary. If you are simply wanting a 'distribution group', then in VPOP3 add the users to a [Distribution List](#) instead of adding them to a group. Note that groups cannot be emailed to from externally: They are only accessible by local users.

A user can be a member of a **Primary Group**. This group allows you to override user settings by group if you wish. The Primary Group has settings such as permissions which can override individual user's settings. This means that you can change the settings for a group of users in one action rather than

individually. However, note that the User [Bulk Edit](#) option may achieve a similar result and be easier to understand in many cases. A user can only be in one **Primary Group**.

A user can be a member of multiple **Secondary Groups**. **Secondary Groups** do not allow you to override user settings but are used for permissions for IMAP4 folder sharing (and may be used for other permissions in the future).

To create a new Group, press the **New** button. To delete a group press the **Delete** button. To edit a group you edit the entries in the table directly. You do not need to 'Submit' any changes on this page, they occur immediately.

If you hover over a cell in the table, the text at the bottom of the screen will give you information about that setting.

Some of the controls are three-state checkboxes. In these cases, if the checkbox is checked as normal, then all members in the group will be made to have this setting set; if the checkbox is clear, then all members will be made to have this setting unset, and if the checkbox is greyed, then all members in the group can have their own individual setting (that particular setting is not affected by the group configuration).

- **Name** - this is the Group name. It cannot be the same as any user or list. When the group is used as a distribution, this is the part of the email address to use before the @ symbol.
- **Enabled** - if this is checked, the group's users are enabled. If it is not checked, then the users are disabled and will not be able to access VPOP3. We have seen this feature used in a school environment where pupils' accounts are in groups by form, and the forms who are meant to be using computers are enabled as appropriate.
- **User Count** - this is a count of how many users are in this group (readonly).
- **Force** - if this is checked, then all users in the group will have the assigned settings, and they cannot be changed individually. If this is not checked, then new users in this group will have the group's settings, but they may then be changed individually.

The remaining options in the table relate to user settings which can be configured by group options. Click on the option name to see it in the user's settings.

- [In Everyone List](#) - if this option is checked, then group members will be put into the "Everyone" list.
- [Allow Sending Internet Mail](#) - if this option is checked, then group members can send outgoing email. If it's not checked, then they will be blocked from sending outgoing mail (note that requiring SMTP authentication is recommended if you want to enforce sending limits).
- [Allow Receiving Internet Mail](#) - if this option is checked, then group members can receive incoming email. If it's not checked, then incoming email to them will be treated as if the recipient was unrecognised.
- [Monitor](#) - if this option is checked, then messages to members of this group will be [Monitored](#).
- [Admin](#) - if this option is checked, then the group's members will be administrators.
- [Max Outgoing Size](#) - if this option is set to 0 (zero), then there is no group limit on the size of messages, but if it is set to a non-zero value, then that is the maximum outgoing message size that the group members can send (in kB). This does not limit internal messages, just outgoing ones.
- **Reply Address** - this option lets you set an "Change outgoing mail sender address" option for a whole group of users at once. If you specify a normal email address, then that email address will be used for all members of the group, but if you use an address starting with a *, such as *@mydomain.com, then the * will be replaced with the username of the user

5.6.9 Header Processing

The VPOP3 Header Processing options tell VPOP3 how to inspect and change message headers generally. This is not used for routing incoming POP3 messages (see Mail Collectors -> [POP3 Routing](#)).

- [Receipts/Urgent Messages](#) - How VPOP3 inspects message headers to generate automated receipts, or to trigger an urgent connection
- [Global Header Modifiers](#) - How VPOP3 changes the headers of outgoing messages

5.6.9.1 Receipts/Urgent Messages

The Receipts/Urgent Messages settings tell VPOP3 when to generate automated receipts and when to trigger an 'urgent' connection outside of the normal [connection scheduling](#).

- [Urgent Messages Tab](#)
- [Receipts Tab](#)

5.6.9.1.1 Urgent Messages

To get to this page, go to Settings → Header Processing → Receipts/Urgent Messages → Urgent Messages tab

Header Processing Show Hints

Reset Defaults Submit

Urgent Messages Receipts

Urgent Messages

VPOP3 can be configured to detect that messages are urgent and to automatically trigger a connection when an urgent message is sent. VPOP3 does this by scanning the message headers looking for one of the specified header fields below.

(NB there is no standard header field defined to indicate urgent messages, so these field definitions may need changing, depending on which email client you are using)

Connect Immediately for Priority Messages

Priority Header fields:

- Priority:Urgent
- X-Priority:Highest
- X-Priority:1
- X-MSMail-Priority:High

VPOP3 can inspect messages which are put into the [VPOP3 Outqueue](#), and trigger an immediate connection if an 'urgent' message is sent, without having to wait for the next scheduled connection. Note that when it does this, VPOP3 will send all waiting messages, not just the urgent messages.

As there is no standard header field defined to indicate an 'urgent' message, VPOP3 allows customisation of the headers to detect. The defaults (shown above) work with most common email clients.

The **Connect Immediately for Priority Messages** option tells VPOP3 to connect immediately if an outgoing message is sent with a message header which matches one of the **Priority Header fields**.

The **Priority Header fields** are checked, the field data is searched for using a case sensitive substring match. For instance, the above checks would match **X-Priority: 1 (important)**, because the **X-Priority: 1** check would match the **1** data in the header.

5.6.9.1.2 Receipts

To get to this page, go to Settings → Header Processing → Receipts/Urgent Messages → Receipts tab

Header Processing Show Hints

Reset Defaults Submit

Urgent Messages **Receipts**

Receipt Message Generation

VPOP3 is capable of generating two different types of 'Receipt' message. The first is a normal 'Delivery Receipt'. This is generated when an appropriate message is downloaded to a user's email client (it does *not* indicate that the message has been read). The second is a 'Transmission Receipt'. This is generated when an outgoing message is sent by VPOP3 onto the Internet.

Delivery Receipt Header fields:
(clear the box to disable delivery receipt generation)

Return-Receipt-To

Only generate Delivery Receipts for Local Messages

Transmission Receipt Header fields:
(clear the box to disable Transmission Receipt generation)

Only generate Transmission Receipts to local users

Don't send Transmission Receipts when LAN Forwarding

If VPOP3 sees a message header containing any fields in the **Delivery Receipt Header fields** box, then it will send a message to the address in that header field when the message is delivered to a user's email client. If you don't want VPOP3 to generate a delivery receipt, simply clear this box.

The **Only generate Delivery Receipts for Local Messages** option tells VPOP3 to only generate these receipts to local addresses, not to external email addresses.

If VPOP3 sees a message header containing any fields in the **Transmission Receipt Header fields** box, then it will send a message to the address in that header field when the message is sent to another SMTP mail server. If you don't want VPOP3 to generate a delivery receipt, simply clear this box.

The **Only generate Transmission Receipts to local users** option tells VPOP3 to only generate these receipts to local addresses, not to external email addresses.

The **Don't send Transmission Receipts when LAN Forwarding** option tells VPOP3 not to send transmission receipts when VPOP3 sends the message using LAN forwarding, but only to send them when it sends a message out to a remote mail server (SMTP relay server/smarthost, or MX mail server)

As there is no standard for header fields to request a receipt, you can customise the header fields which VPOP3 should look for here. **Return-Receipt-To:** is a common header field to indicate that a receipt is wanted, but there are others. If you look at the full headers of an example message which you have sent when asking for receipts, then that may show you which header field to look for.

You can use 'From' in either of these boxes if you want VPOP3 to *a/ways* generate a receipt, but you should be careful when using this option.

5.6.9.2 Global Header Modifiers

To get to this page, go to Settings → Header Processing → Global Header Modifiers

The screenshot shows the 'Global Header Modifiers' configuration page in the VPOP3 admin interface. The page title is 'User Global Header Modifiers'. A text area contains the setting 'X-Organisation: Paul Smith Computer Services'. Below the text area, there is explanatory text: 'Global header modifiers modify the message headers of outgoing messages. You can specify any message header fields that you want modified or added to outgoing messages. Specify them as **Field: Data** to add or modify a header field. Use simply **Field:** to remove that field from the header. The following special values can be used in the **Data** portion of the setting:

- %O = email address of message originator
- %N = text name of message originator
- %% = the '%' character

A 'Submit' button is visible at the top right of the settings area.

Global header modifiers are applied to all outgoing messages. These aren't needed, but there may be cases where you want to add them. The most common one would be an Organization/Organisation/X-Organisation header as in the example above.

You should be careful about adding 'random' header fields as they may mean something to other software and cause interoperability problems.

If you are going to use this facility, you should probably read and understand at least sections 1 to 3.2 of [RFC 5322](#) to understand how message headers are formatted.

[RFC 2076](#) is a useful list of common message headers. It is a bit old, but still useful. Note that header fields beginning with 'X-' are custom headers and should not have any important meaning.

To specify a header modifier, type it into the **Global Header Modifiers** box as it will appear in the final message header. You should put the header field name, followed by a ':' followed by the header field data, as described in RFC 5322.

If you have a header modifier, and that header field already exists in the sent message, then VPOP3 will modify the existing header field. If the header modifier has no data section, then the existing header field will be deleted (this may be useful for redacting data added by email clients, but be aware of possible interoperability issues). If you have a header modifier and the header field does not exist in the sent message, then VPOP3 will add that header field.

You can use **%O** in the field data to insert the email address of the message sender, or **%N** to insert the text name. Use **%%** to insert a single percent character.

5.6.10 Legacy Extensions

To get to this page, go to Settings → Legacy Extensions

VPOP3 Legacy Extensions Show Hints Submit

External Router

The External Router is a program which is run on each incoming POP3 message to determine who the message should be sent to, instead of the default recipient calculated by VPOP3. It is often used for tasks such as virus scanning, attachment filtering, etc.

Command :

Timeout : 60 seconds

Ignore Return Code (otherwise a non-zero return code causes an error message)

OutMail Pre-processor

The OutMail Pre-Processor gets run on messages which VPOP3 receives via SMTP. It is normally used for processing outgoing messages, but can also be used for processing incoming and local messages if the appropriate checkbox is ticked below.

Command :

Timeout : 60 seconds

Ignore Return Code (otherwise a non-zero return code causes an error message)

Run OutMail Pre-processor for incoming/local mail

SMTP Client Processor

The SMTP Client Processor gets run on messages just before they go through the SMTP Client for 'SMTP Relay' outgoing mail.

Command :

Timeout : 60 seconds

Ignore Return Code (otherwise a non-zero return code causes an error message)

Post-Connect Command

The Post-Connect Command gets run immediately after VPOP3 connects to the Internet

Command :

Timeout : 54 seconds

Pre-Disconnect Command

The Pre-Disconnect Command gets run immediately after VPOP3 connects to the Internet

Command :

Timeout : 10 seconds

VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23 | Idle | In: 49290 | Out: 0

Legacy Extensions are a way that VPOP3 v2 and earlier could be extended to alter their behaviour. Current installations of VPOP3 should use [Scripts](#) or Plugins instead. Legacy Extensions were standalone command-line executable files (EXE files) which VPOP3 ran on certain events and possibly sent data to and received data from to alter its behaviour. These were slow and often unreliable, so the

extension mechanisms were altered in later versions of VPOP3, but the options are still available for backwards compatibility.

We do not recommend that anyone use these mechanisms for creating new extensions for VPOP3. Instead use scripts or plugins as appropriate. (Scripts use the Lua scripting language, Plugins are created as Windows DLLs)

If these options are blank, then VPOP3 will skip the extension hook.

- **External Router** - when VPOP3 downloaded a message using POP3 and was about to deliver it to a user, VPOP3 passes the message content and data about the message (recipient, sender etc) to a program called an 'External Router' program. The output of this program will determine what VPOP3 should do with the message.
- **OutMail Pre-processor** - when VPOP3 received a message using SMTP, it runs the OutMail Pre-processor program with the message data as input, and receives modified message data as an output. If **Run OutMail Pre-processor for incoming/local mail** is checked then this program is run for all SMTP messages, otherwise it is only run for messages to external recipients.
- **SMTP Client Processor** - when VPOP3 is about to send a message out via an SMTP relay Sender, VPOP3 passes the message to the **SMTP Client Processor** program.
- **Post-Connect Command** - VPOP3 runs this command just after it makes a **Connection** to the Internet. This used to be commonly used for triggering other programs to use the same dial-up connection session before the days of always-on connections.
- **Pre-Disconnect Command** - VPOP3 runs this command just before it disconnects a **Connection**. This used to be used to tell other software to stop using the dial-up connection which VPOP3 had initiated.

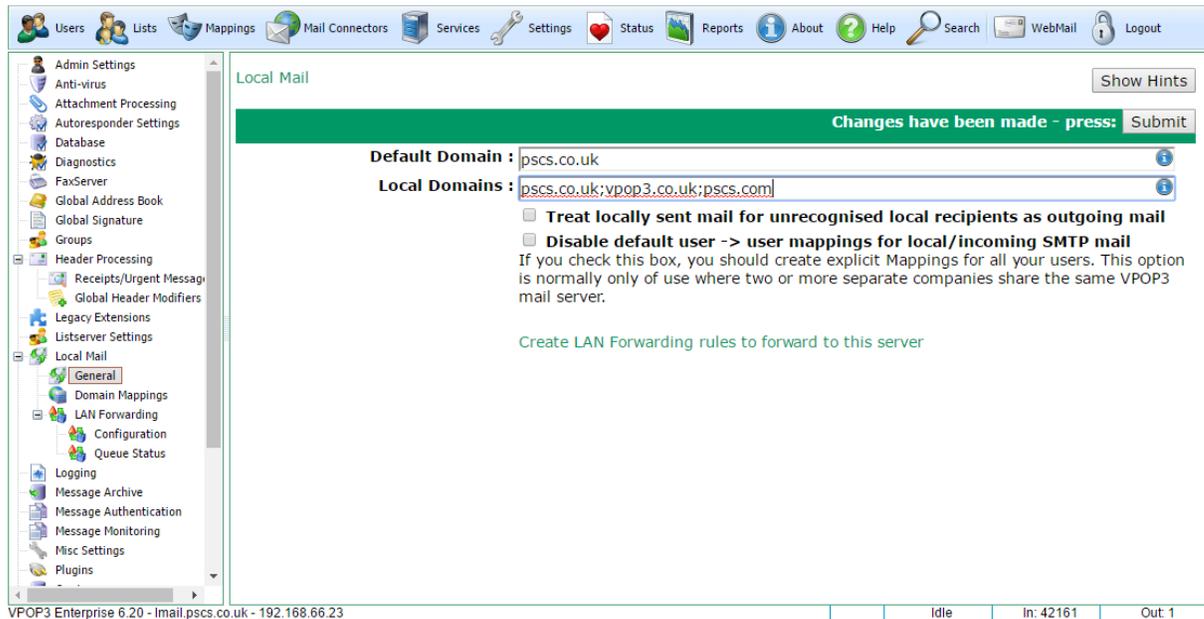
5.6.11 Local Mail

The VPOP3 Local Mail options tell VPOP3 how to handle mail within your local network. This includes mail between local VPOP3 users and mail to other local SMTP servers (eg other VPOP3 servers, Microsoft Exchange Server, or Linux mail servers).

- [General](#) - How VPOP3 handles mail between local VPOP3 users
- [Domain Mappings](#) - How VPOP3 maps domain names between 'internal' domains and 'external' domains (not usually needed and for advanced users only)
- [LAN Forwarding](#) - How VPOP3 sends mail to other local SMTP mail servers.

5.6.11.1 General

To get to this page, go to Settings → Local Mail → General



This page lets you set how local mail is handled. Local mail is mail from one local user to one or more other local users. If a message is sent to local users and remote users, then the local recipients will be handled according to the settings here, and remote recipients will be treated as outgoing mail.

The **Default Domain** is the domain name to be added to addresses which don't have a domain explicitly defined. For instance, if there is a user called 'bob' who sends a message from VPOP3's Webmail, then the sender address will default to *bob@<default domain>*. So, this should be your 'main' domain. This can be overridden for specific instances if necessary, but in most cases, an organisation will have a single main domain, so defining it here simplifies administration.

Note - the Default Domain is a SINGLE domain. If you specify more than one domain here, you WILL have problems!

The **Local Domains** setting indicates which domains VPOP3 should treat as for local users. So, mail addressed to the domain(s) specified here will be handled internally by VPOP3 and will not go out to the Internet. VPOP3 checks this for all mail it receives using SMTP, so that means locally sent messages or messages which are received through an incoming SMTP feed. This can be overridden for specific addresses using [*REMOTE mappings](#). So, in the above screenshot, mail for anyone@pscs.co.uk, anyone@vpop3.co.uk and anyone@pscs.com will be handled internally by VPOP3. You can use full email addresses or wildcards here if you wish, but that is rarely appropriate. *@pscs.co.uk is equivalent to pscs.co.uk, but the latter is more efficient.

If the **Treat locally sent mail for unrecognised local recipients as outgoing mail** option is checked, then if a local user sends a message to an email address on a local domain, but that address does not exist either as a User, List or Mapping, then VPOP3 will put it into the Outqueue to be sent to the Internet. This is sometimes needed, but not often, so make sure it is really what you need. If there is not another mail server which will handle these addresses, then the messages will just come back into VPOP3 (eg through a catch-all account) and cause errors. It is usually better to specifically list remote email addresses using [*REMOTE mappings](#) if necessary.

The **Disable default user -> user mappings for local/incoming SMTP mail** option can be used if you want to explicitly define Mappings for email routing. Normally, a user will have an automatic email address of <username>@<local domains>, but this option removes that automatic email address mapping. So, if you have a VPOP3 user called *bob* and your Local Domains is set to *example.com*, if you don't do anything else, local or incoming SMTP mail for *bob@example.com* will be delivered to the *bob* mailbox. In most cases this is desirable, but in some cases it may not be. For instance, if you have several domains with different users with the same "user" part of their email address.

For example, if you have two domains *example.com* and *example.net* and two email addresses *bob@example.com* and *bob@example.net* where mail to those addresses goes to different mailboxes *bob1* and *bob2*. You can create [Mappings](#) of *bob@example.com* -> *bob1* and *bob@example.net* -> *bob2*. That will achieve what you need, but if the **Local Domains** is set to *example.com;example.net*, mail for *bob1@example.com* and *bob1@example.net* will also go into the *bob1* mailbox, and so on, which may be undesirable. By checking the **Disable default user -> user mappings** option, you make it so that only the explicit Mappings will take effect.

The **Create LAN Forwarding rules to forward to this server** link will let you create a set of rules which you can import to another VPOP3 server so that it will [LAN Forward](#) messages to users on this server. You can use this to help configuration if you have two (or more) VPOP3 servers which you want to send messages between using LAN forwarding.

5.6.11.2 Domain Mappings

To get to this page, go to Settings → Local Mail → Domain Mappings

From Domain	To Domain
bbb.com	ys.com

This page is for an advanced setting. It is rarely needed, and in most cases where you think it might be needed, it probably isn't. Really.

Generally the only time it is needed is if you have a legacy configuration where you have a different email domain inside your company than is used from outside to contact you.

For instance, you may use the fictional domain '*internal*' inside your company, and the real domain '*example.com*' outside. So, to email a local user '*fred*' from another local user, you would send to

'fred@internal', but to email the same user from outside your company you would use 'fred@example.com'. In this case you would set up your internal email client to know that your email address is something like 'bob@internal', so that when internal users reply to your messages they will go to the @internal address. Obviously this causes problems if you send outgoing mail, the external recipient will see the reply address as being 'bob@internal' rather than 'bob@example.com'.

You *could* create two 'identities' in your email client and choose the appropriate one when sending messages, but mistakes may happen and you may occasionally use the wrong address.

That is what **Domain Mappings** are to help with.

To help with the above example situation, you would press **New** to add a new Domain Mapping, then in the **From Domain** column, put 'internal', and the the **To Domain** column, put 'example.com'.

Then, when you send a message, VPOP3 will look through the message headers and change any email addresses in the **From Domain** to be in the **To Domain**. This includes the *To* and *Cc* etc as well as the *From* and *Reply-To* headers, so if bob@internal sends a message to kate@customer.com and CCs fred@internal, Kate will see that it came from bob@example.com and was sent to kate@customer.com and Ccd to fred@example.com.

If you are setting up a new system, we strongly recommend that you do NOT try to be clever and use this feature, it will cause confusion and extra complexity. Instead, simply use the same email addresses internally and publicly.

5.6.11.3 LAN Forwarding

LAN Forwarding is the term we use for sending mail from your VPOP3 mail server directly to other SMTP servers. It is called 'LAN Forwarding' because it is usually performed on a local network, but it can often be used across the Internet as well.

LAN Forwarding is different from normal outgoing mail because:

- you have to tell VPOP3 which mail server to send the messages to. It cannot use DNS MX record lookups to find the appropriate server
- VPOP3 assumes the remote server is always available. [Connection scheduling](#) is not used with LAN forwarding.
- the LAN Forwarding queue is separate from the normal outgoing message queue.

LAN forwarding is mainly configured in the [Settings](#) → [Local Mail](#) → [LAN Forwarding](#) → [Configuration](#) page and you can monitor the LAN Forwarding queue in the **Queue Status** page.

You can also set up LAN forwarding in most places where you can specify a target email address, such as in distribution lists or user forwards/assistants. To do this specify the target email address as:

```
"SMTP:<email address>@[<user>:"<pass>"@]<server>:"[<port>]
```

<user>:<pass>@ and :<port> are optional

So, a simple target would be:

```
SMTP:bob@example.com@192.168.1.1
```

This will tell VPOP3 to send the messages to bob@example.com on the SMTP server at 192.168.1.1, not using authentication and on the standard SMTP port 25

A more complex target would be:

SMTP:bob@example.com@fred:mypass@192.168.1.1:587

This will tell VPOP3 to send the messages to bob@example.com on the SMTP server at 192.168.1.1, logging on using the username 'fred' and the password 'mypass', and sending on the SMTP submission port 587

5.6.11.3.1 Configuration

To get to this page, go to Settings → Local Mail → LAN Forwarding → Configuration

The screenshot shows the 'LAN Forwarding' configuration page. At the top, there is a navigation bar with icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, and Search. On the left, a sidebar menu lists various settings categories, with 'Local Mail' expanded to show 'LAN Forwarding' and 'Configuration' selected.

The main content area is titled 'LAN Forwarding' and includes a 'Show Hints' button. Below this is a table with columns: Cond, Address, Server, User, Pass, Rewrite Address, and Matches. The table contains four rows of data:

Cond	Address	Server	User	Pass	Rewrite Address	Matches
	blob@blobby.com	192.168.66.70:25	paul	*****		1
SMTP	*@aaaaa.com	192.168.99.99				4
	aaa@aaa.com	1.2.3.4	paul	*****		0
	mike@pscs2.co.uk	192.168.66.101				151

Below the table is a section titled 'Configure Server Address Verification for Wildcards' with the following settings:

- LAN Forwarding Retry Frequency: 10 minutes
- LAN Forwarding time before failure: 72 hours
- Maximum number of LAN Forwarding threads: 11
- LAN Forwarding thread rules: (empty text box)

Additional options include:

- Send failure reports for failed LAN forwarding messages
- Allow LAN forwarding addresses without a specific domain (page must be submitted before changes to this setting take effect)

The top section of the page shows the LAN Forwarding Rules which are defined. These tell VPOP3 which addresses to send to other local SMTP servers.

VPOP3 goes through the rules in order until one matches. This can be important if you use wildcards. You can reorder the rules by simply selecting the appropriate rule(s) in the table, and dragging them up or down to the correct position.

Adding a rule

To add a new rule, press the Add Row button. This brings up a window where you can enter the details

Add LAN Forwarding Entries

Addresses :

Target SMTP Server :

Target SMTP Port :

SMTP Username :

SMTP Password :

Rewrite Address :

In the **Addresses** box you can enter one or more original email addresses which will be forwarded to the same server. Enter one address per line. You can use DOS style wildcards (* and ?) in the addresses. If you use ~ as the username part of the address (eg ~@domain.com) then this rule will only be checked after all other addresses (users, mappings, lists, specific LAN forwarding addresses etc) have been checked and haven't matched.

Normally, the addresses have to be full email addresses. Note that they do NOT have to be addresses in your [Local Domains](#) or [Accepted Domains](#). If you check the box "**Allow LAN forwarding addresses without a specific domain**" box, then you can enter just the username part of the email address. In that case, these entries will match that username at *any* of your Local Domains or Accepted Domains as appropriate.

In the **Target SMTP Server** box you can enter the target SMTP server where messages for the specified addresses are to be sent

In the **Target SMTP Port** box enter the target SMTP port (usually 25 or 587). Note that you cannot use SSL (eg port 465) when using LAN forwarding

In the **SMTP Username** and **SMTP Password** boxes, you can optionally enter a username & password which VPOP3 should use when logging onto the remote server. If these are blank then SMTP authentication is not used.

In the **Rewrite Address** box you can optionally enter an address which VPOP3 should redirect the messages to. If you use *@... in the **Address** box, then you can also use *@... in the **Rewrite Address** box and VPOP3 will use the original username from the recipient, but will change the domain. If you leave it blank, then VPOP3 will use the entire original recipient address

Deleting a rule

Select the rule(s) which you want to delete and press the Delete Row button.

Editing a rule

To edit a rule, simply double-click on the value you want to change. This gives a slightly different box to adding a rule. Here you can only specify a single address. There is also the option to specify conditions where this LAN Forwarding rule will act

Edit LAN Forwarding Entry

Conditions : All
 POP3
 SMTP
 [blurred]
 [blurred]

Address :

Target SMTP Server :

Target SMTP Port :

SMTP Username :

SMTP Password :

Rewrite Address :

The possible conditions are:

- All - for all the time
- POP3 - for all POP3 collected mails
- SMTP - for all mail received using SMTP
- the various 'Mail Collector' names for the rule to only act on messages downloaded using POP3 from the specified collector

Configure Server Address Verification for Wildcards

This lets you configure how VPOP3 can check that an email address on an incoming SMTP message is valid at the onward server before deciding whether to accept or reject it. This can be useful if you are using VPOP3 as a backup SMTP server, so it will only accept mail for valid recipients if the final destination mail server is still active. If the final destination mail server does not respond, then VPOP3 will accept the mail in any case as it has no way of knowing whether the recipients are valid or not

[Configure LAN Forwarding Server Address Verification for Wildcards](#)

Other Options

- **LAN Forwarding Retry Frequency** - this tells VPOP3 how often it should retry failed messages. If this is set too high, then there may be unacceptable delays if the onward mail server was down temporarily and has now recovered. If it is set too low, then it will place excessive load on the VPOP3 server
- **LAN Forwarding time before failure** - this tells VPOP3 how long it should try failed messages for before it fails then and sends a failure notification to the original sender
- **Maximum number of LAN Forwarding Threads** - this tells VPOP3 how many messages it should try to send at once to the onward server(s). Setting it too high will place excessive load on VPOP3 and on the onward server, but setting it too low may mean that messages don't get delivered in a timely fashion if you have large numbers of messages going through VPOP3
- **LAN Forwarding thread rules** - see below
- **Send failure reports for failed LAN Forwarding Messages** - if this is turned off, then any messages which can't be delivered to the onward server will be failed after the LAN Forwarding time before failure time and NO error message will be sent to the original sender. The normal behaviour is for this to be turned on, and the messages will be failed after the specified time, but a message will be sent back to the original sender to say that the message delivery failed
- Allow LAN forwarding addresses without a specific domain - see the **Addresses** section above in **Adding a rule**

LAN Forwarding Thread Rules

LAN Forwarding Thread Rules are useful if you have one copy of VPOP3 forwarding to several different mail servers. It lets you specify the maximum number of sending threads for each onward server.

Enter the rules as a set of space separated items, with each item being <server>-<max threads>

For instance 192.168.1.1-10 192.168.2.1:1025-5

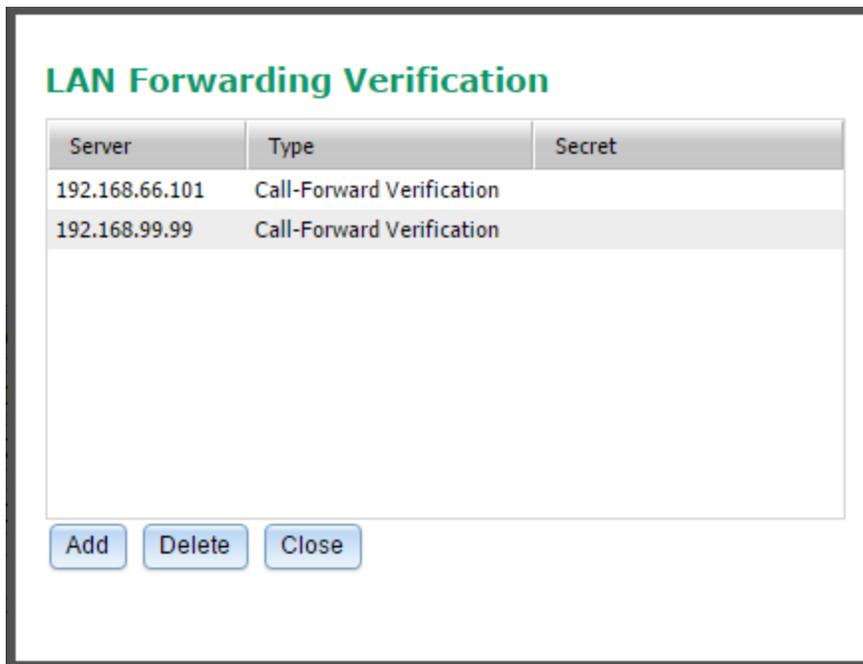
will mean that VPOP3 will only send up to 10 messages at once to the 192.168.1.1 server, and up to 5 messages at once to the 192.168.2.1 server on port 1025.

The Maximum number of LAN Forwarding threads setting takes precedence, so if that was set to 5 in this example, then VPOP3 would only send up to 5 messages at once to the 192.168.1.1 server, and it would only send up to 5 messages at once overall, so it might send 3 messages to 192.168.1.1 and 2 messages to 192.168.2.1

Any servers which are not specified in these rules will have no limit (other than the overall maximum number of threads)

5.6.11.3.1.1 Configure LAN Forwarding Server Address Verification for Wildcards

To get to this page, go to Settings → [Local Mail](#) → [LAN Forwarding](#) → [Configuration](#) and press the **Configure Server Address Verification for Wildcards** button.



When you configure VPOP3 to LAN Forward to another mail server and specify a wildcard address, such as `*@mydomain.com`, it is unlikely that every possible email address will be valid at the onward mail server. If VPOP3 attempts to forward undeliverable messages, and the onward mail server rejects them, VPOP3 will have to generate a delivery failure report for that message, which can cause 'backscatter'. Because of this, it can be useful to have VPOP3 verify that the email address is allowed before it accepts the message in the first place.

That is what the **LAN Forwarding Verification** facility is for. When VPOP3 receives a message which it is configured to LAN forward using a wildcard (containing `*`, `~` or `?`) LAN Forwarding rule, then it can perform an action to verify that the address is allowed before accepting the incoming message.

Normally, VPOP3 does not perform any type of verification when it receives an incoming message, but you can create rules by telling VPOP3 how to check with the onward mail server whether the address is valid. To do this, press the **Add** button and put the server address (as defined in the LAN Forwarding configuration) in the **Server** column. Choose the verification type in the **Type** column, and, if you are using Minger verification, put the Minger shared-secret in the **Secret** column.

The two types of verification that VPOP3 supports are:

- Call-Forward verification
- Minger verification

Call-Forward verification

With Call-Forward verification, VPOP3 tries to make a connection to the onward server to start sending a message to the recipient to see if the onward server will accept messages to that recipient. VPOP3 won't actually send a message, but it tries to send a message from a blank return-path to the specified recipient. This can fail if the onward mail server supports [BATV](#) or otherwise does not allow messages from a blank return-path. It can also make some servers become suspicious of VPOP3 because it can appear to be trying invalid recipients (when there are incoming messages for incoming recipients), so you may need to tell the onward mail server to trust VPOP3.

Call-Forward verification should work with most SMTP servers as long as they are configured to allow the blank return-path messages from VPOP3 without blocking it.

If VPOP3 cannot connect to the onward mail server at all (eg it is not running), then VPOP3 remembers if it has recently seen that the recipient was unknown, if it was then it will reject the incoming message, otherwise the recipient will be accepted (including if the recipient has not been checked before).

Minger verification

With Minger (Mail pINGER) verification, VPOP3 connects to a Minger service on the onward server to verify the address. Minger is a protocol specifically designed for verifying email addresses for this type of purpose. It is not widely supported, but [VPOP3 supports it](#), as do several other mail servers. The Minger server has a 'secret' (password) to prevent unauthorised use, which you need to tell this verification feature about in the **Secret** column.

If the onward server supports it, Minger verification is the best option to use as it was designed specifically for this purpose.

Again, if VPOP3 cannot connect to the onward mail server at all (eg it is not running), then VPOP3 remembers if it has recently seen that the recipient was unknown, if it was then it will reject the incoming message, otherwise the recipient will be accepted (including if the recipient has not been checked before).

5.6.11.3.2 Queue Status

To get to this page, go to Settings → [Local Mail](#) → [LAN Forwarding](#) → Queue Status

LAN Forwarding Queue Show Hints

Sender	Target Server	Recipient(s)	Subject
<input type="checkbox"/> support@pccs.co.uk	192.168.99.99	test@aaaaa.com	test 1 2 3

This page shows messages in the [LAN Forwarding](#) queue which are waiting to be sent on to other SMTP mail servers.

The four columns in the table show:

- **Sender** - this is the email address of the person who sent the message
- **Target Server** - this is the name/IP address of the mail server where the message will be sent. This is obtained from the configuration entry which put the message into the LAN Forwarding Queue

- **Recipient(s)** - this is a list of email addresses which the message has to be sent to. Note that if the message has been sent to some of the original recipients, only the remaining recipients will be listed here
- **Subject** - this is the message subject. This is useful for finding a particular message, but not used in the actual LAN forwarding process itself

The list is limited to 100 entries, so if there are more than 100 entries, only the first 100 will be displayed.

You can delete messages from the queue by checking the box to the left, and pressing the **Delete Messages From Queue** button. Note that you cannot remove any messages which are being sent at the same time as you press the button.

If you press the **Pause LAN Forwarding** button, then VPOP3 will pause the LAN forwarding background tasks until you press the **Resume LAN Forwarding** button (which is hidden unless it is paused).

To refresh the list, press the **Refresh Queue View** button.

5.6.12 Logging

To get to this page, go to Settings → Logging

The screenshot shows the VPOP3 Administration Console interface. The left sidebar contains a tree view of settings categories, with 'Logging' selected. The main content area is titled 'Administrative Logging' and includes a 'Show Hints' button. Below this is a green bar with a 'Submit' button. The 'Activity Summary Reports' section contains several checkboxes: 'Send daily summary logs to Main Administrator' (checked), 'Show Idle Accounts in the Summary log' (checked), 'Generate HTML format summary messages' (checked), 'Keep raw Summary log files in the SUMMARIES directory' (checked), and 'Keep MAIL.LOG files in the SUMMARIES directory' (unchecked). The 'Security Logging' section has a checkbox for 'Security Log contains Successful logons' (checked). The 'Other Logging' section has a checkbox for 'Write all status window messages to CONNECT.LOG' (unchecked). The 'Historical Logging' section has a checkbox for 'Enable Historical Logging' (checked) and a text input for 'Store Historical Logging Data for' set to 5000 days. The 'Log Database Status' section indicates the log database is currently active and the queue holds 0 items.

This page lets you configure some administrative logging options. Note that this is different from diagnostics logging which is managed on the [Diagnostics](#) page.

Activity Summary Reports

VPOP3 can send the administrator a daily usage report showing how many messages have been received & sent by the various users. This is enabled with the **Send daily summary logs to <xxxx>**. You can choose who the report goes to. If you choose **Main Administrator** the report goes to the user designated as the Main Administrator in the [Admin Settings](#). The email you receive will have the subject "VPOP3 Daily usage Summary for <date>"

If the **Show Idle Accounts in the Summary log** option is checked, the usage report will show accounts which haven't been logged into for at least a day.

If the **Generate HTML format summary messages** option is checked, the usage report will be sent in HTML format as well as plain text. The format is still the same, but it uses HTML to indicate that the font should be fixed-width and so on, which helps with formatting in some email clients which display plain text messages in a variable-width font.

The **Keep raw Summary log files in the SUMMARIES directory** option tells VPOP3 to copy the raw data which is used to generate the report in the **SUMMARIES** directory inside the VPOP3 directory, otherwise it is deleted after the report is generated. This raw data may be useful if you wish to perform your own analysis - [the file format is described here](#).

As well as the daily summary log, VPOP3 keeps a **MAIL.LOG** file which contains more information about sent/received messages. This is renamed daily to **MAILLOG.MON**, **MAILLOG.TUE** etc up to **MAILLOG.SUN**, then, the next week these files are overwritten. If the **Keep MAIL.LOG files in the SUMMARIES directory** option is checked, then VPOP3 will copy these files into the **SUMMARIES** directory as well.

Security Logging

VPOP3 logs all failed login attempts to a log file called **SECURITY.LOG** in the VPOP3 logging directory. This can be useful for diagnosing login problems because it contains more details of why a login failed than the normal login response does. The login response is a generic "Login Failed" to avoid helping an attacker, but the SECURITY.LOG file will indicate whether the problem was with the [password](#), or [permissions](#) or [IP access restrictions](#) etc.

If the **Security Log contains Successful Logons** box is checked, then the SECURITY.LOG file will also show successful logins.

Other Logging

VPOP3 writes a brief summary of connections to a file called **CONNECT.LOG** (eg time online, how many messages were downloaded etc). If **Write all status window messages to CONNECT.LOG** is checked, then all data displayed on the [Status Monitor activity log](#) or the [Server Status](#) page will also be written to the CONNECT.LOG file.

Historical Logging

The **Historical Logging** option in VPOP3 makes VPOP3 write a summary of all messages and sessions to a database table. This can then be used for some reports. However, this logging does add load to the server and take up disk space, so it is optional.

The **Enable Historical Logging** option turns this facility on or off.

The **Store Historical Logging Data for x days** option tells VPOP3 how many days it should keep the data for. Obviously the larger this setting is, the more disk space will be used.

The **Log Database Status** section shows whether the Historical Logging database is active and how many entries are waiting to be written to the database. (Writing to the database is a low priority background task).

5.6.13 Message Archiving

Message Archiving lets VPOP3 keep a copy of all sent/received messages for future reference.

- [General Tab](#)
- [Search Tab](#)
- [Offline Tab](#)
- [Maintenance Tab](#)

Archived messages can be stored on a local, networked or external hard drive. If the store location is unavailable, then VPOP3 will queue up the messages locally so that they will not be lost.

The archive can be searched on the **Search** tab using various parameters, and you can copy the found messages back into a user's mailbox.

You can choose to move old messages out of the main archive store into a ZIP file (which can be copied to DVD, external HDD etc) on the **Offline** tab. If you move messages to ZIP files, then the search can still find the message and tell you which ZIP file is needed to access the message.

Note for VPOP3 Enterprise Users

Note that the VPOP3 message archive is *not* the same as, for instance, the Microsoft Outlook archive function. The VPOP3 message archive stores all sent/received messages for later access, for instance in case of disputes. The Microsoft Outlook archive lets you move older messages to another location where they can still be accessed by the user. There is no equivalent to the Microsoft Outlook archive function in VPOP3, because there is no point moving the messages to another location which is still on the mail server; that would not give any benefit to performance, or storage requirements, so would just complicate things for the user, with no benefit to the user. You can still use the 'archive' function of your email client to move messages out of the mail server and into a local message store - that will reduce storage requirements on the server, at the expense of needing to be backed up separately and of not being accessible to all devices or shareable. If you want old messages to be backed up with the server, accessible to all devices and shareable, they have to be stored on the mail server, which means they have to take up storage space on the mail server; there is no way to have them stored on the mail server but not take up space on the server.

5.6.13.1 General

To get to this page, go to Settings → [Message Archiving](#) → General

VPOP3 Enterprise 6.20 - Imail.pscs.co.uk - 192.168.66.23

Idle In: 39326 Out: 0

This page tells VPOP3 how to archive messages.

The **Archive Messages** checkbox tells VPOP3 whether or not to archive messages. There are no options to tell VPOP3 which messages to archive, it will archive all sent/received messages, or none (with the exception of being able to not archive messages which are detected as spam - see below).

The **Main Archive Store Directory** option tells VPOP3 where to store archived messages. Messages are stored as individual files in the specified directory and subdirectories. You can specify a local drive (either internal or external) or a network drive here. If you specify a network drive you must use the **UNC** naming convention - `\\server\share\path`. You can **NOT** use mapped drives here. This is because VPOP3 runs as a Windows service, and services cannot use mapped drives.

If you change the Main Archive Store, then VPOP3 will automatically move messages from the previous store(s) to the new one if the previous stores are still accessible. This may take some time, so you shouldn't make the old store inaccessible until it is empty.

The **Username/Password to access Main Store** options let you specify the username/password required to access a network share. Note that because VPOP3 is running as a service, probably as a different Windows user from the currently logged in user, that means that just because the currently logged in user can access the network share does not mean that VPOP3 can, so you need to enter an appropriate username/password here.

VPOP3 will display a message on this page if it cannot write messages to the file share. This message will contain Windows error codes/messages, so if you are unsure what the error message means, searching for it on the Internet will usually give further information.

In the box under the password setting, VPOP3 displays how many messages are in the archive store, and their total size (2.9 million messages and 105GB in the screenshot above). It also displays how many messages are currently queued up to be written to the main store. When VPOP3 processes a message, it saves it to a temporary local location first, and then moves it to the main archive store in the background. This is in case the main store is inaccessible (eg the network share is offline, or an external drive has been unplugged). If this number is large, then it may indicate a problem with accessing the main archive store. Messages which are waiting to be written to the main store are not searchable.

The **Speed up processing of pending messages to main store** option tells VPOP3 to process messages more quickly. This will increase the load on the VPOP3 server, but may be useful if there was a problem accessing the main archive store that has now been fixed.

The **Don't archive spam** option tells VPOP3 not to archive messages which were quarantined. This can be useful to save space if you receive large amounts of spam. Note that if a message is released from the VPOP3 quarantine, then it is added to the message archive as well, but if someone reads a message from the quarantine directly, then that will not be added into the archive.

The **Extra Archive Actions** section lets you define extra actions to perform on moving a message into the archive - for instance copying it elsewhere, or FTPing it to another site, etc. See the Extra Archive Actions topic for more information.

The **Digital Signing Private Key** option lets you specify an RSA private key for archived messages to be signed with. This may be required in some locations to prove that the archived messages have not been tampered with. Note that it can NOT prevent someone tampering with a message and re-signing it, if they have access to the private key.

5.6.13.1.1 Extra Archive Actions

On the Settings → [Message Archiving](#) → General page there is the facility to add **Extra Archive Actions** - this topic documents that feature.



Extra Archive actions are actions which VPOP3 can perform when it is copying messages into the VPOP3 archive main store. They can be used to copy messages to other locations. They are an advanced feature and are not needed for the main VPOP3 archive functionality to work. In fact, if the extra actions do copy the archived messages elsewhere, VPOP3 cannot access those other locations automatically to retrieve messages, so that would have to be performed manually.

The archive actions which are currently available (in VPOP3 7.0) are:

- execute command
- encrypt
- compress
- ftp
- sftp

Each command must be entered on a line of its own, with the appropriate parameters as necessary, described below. VPOP3 processes actions in order from top to bottom, so the output of one action can be used as the input to a later action. For instance, if you want to compress and encrypt a file before FTPing it to a remote server, you could use the **encrypt** action, then feed the output of that to the **compress** action and then feed the output of that to the **ftp** action.

In the syntax descriptions below, items in [] are optional, items in <> replaced with relevant text, items in () indicate possible values, and | separates various possible values.

Any parameters which contain space characters should be surrounded with " quotes. If you want to include quotes in your parameters, use a pair of quote characters, ie ""

Variables

When performing actions, values surrounded by {} are "variable names". These can be generated by VPOP3 or by other actions. VPOP3 will replace these in any action parameters with the variable contents.

You can replace parts of variables by appending :x,y to the variable name, for instance {myvar:1,3} will give you characters 1 to 3 of the myvar variable.

If you want to use { or } characters in your parameters, use {{ or }} instead.

The built in variables are:

- **{tempfn}** - the source filename which VPOP3 is moving to the main store.
- **{fn}** - the target filename which VPOP3 is creating in the main store.
- **{authsender}** - the authenticated sender username (if any) of the message being archived.
- **{subject}** - the subject of the message being archived.
- **{returnpath}** - the return path email address of the message being archived.

In various commands, if the **output** option is specified, then VPOP3 will create a temporary filename and store it in that variable - for instance:

```
output=myfile
```

will create a temporary filename and put it into the **{myfile}** variable. These temporary files are deleted after all archive action process has finished (whether successful or not).

Execute command (cmd)

Execute an arbitrary command-line program or command.

The syntax is:

```
cmd: cmd="<command>" [output=<name>] [ignoreresult=(yes|no)] [timeout=(0-99)]
```

For instance, to copy the source file to a temporary file and store the temporary filename in the variable **{copyfile}** you could use

```
cmd:cmd = "copy ""{tempfn}"" ""{copyfile}"" output=copyfile
```

This will cause a command to be passed to cmd.exe such as: `copy c:`

```
\vpop3\_archive\p12345abcdef.dat c:\vpop3\outqueue\t12345.dat
```

and for the remainder of the archive actions **{copyfile}** will be replaced with **c:**

```
\vpop3\outqueue\t12345.dat
```

The command can be a built-in cmd.exe command, such as COPY or an external program designed to be run from a command-line.

The parameters are:

- **cmd** - the command to run (mandatory).
- **output** - if this is specified a temporary filename will be generated and put into the specified variable for use in **cmd** (optional).
- **ignoreresult** - yes or no (optional - defaults to no) - if the command doesn't return 0 (success) then the action will fail unless **ignoreresult=yes** is specified.
- **timeout** - a number from 1 to 99 seconds (optional - defaults to 60 seconds) - if the command doesn't complete in the specified time the action will fail.

Encrypt

Encrypt a file.

The syntax is:

```
encrypt: [input=<name>] output=<name> [type=(3des|aes256|blowfish|des)] password=<password>
```

For instance, to encrypt the filename in the variable **{copyfile}** to a file in **{encfile}** using **blowfish** encryption you could use

```
encrypt:input=copyfile output=encfile type=blowfish password="my password"
```

The parameters are:

- **input** - the file to encrypt (optional - defaults to {tempfn}).
- **output** - The name of the encrypted file.
- **type** - 3des, aes256, blowfish or des (optional - defaults to blowfish) - the type of encryption to use.
- **password** - the password to use for the encryption.

Compress

Compress a file.

The syntax is:

```
compress: [input=<name>] output=<name> [type=(zip|gzip|bzip2)] password=<password> [filename=<
```

For instance, to encrypt the filename in the variable **{encfile}** to a file in **{compfile}** using **zip** compression you could use. The zip file will contain the message as a file called 'mymessage.dat'.

```
compress:input=encfile output=compfile type=zip filename=mymessage.dat
```

The parameters are:

- **input** - the file to compress (optional - defaults to {tempfn}).
- **output** - The name of the compressed file to be created.
- **type** - zip, gzip or bzip2 (optional - defaults to zip) - the type of compression to use.
- **password** - the password to use to encrypt the file (optional - zip type only)
- **compression** - the level of compression (0 = less compression, quicker, 9 = more compression, slower) (optional - zip & gzip types only)
- **filename** - the filename of the compressed file inside the compressed archive file

FTP

Upload a file using FTP.

The syntax is:

```
ftp: [input=<name>] [ssl=none|ftps|ftpes|implicit|explicit)] [ccc=(yes|no)] host=<hostname> [pas
```

For instance, to ftp the filename in the variable **{compfile}** to the server **myftpserver.com** with VPOP3's target filename you could use

```
ftp:input=compfile host=myftpserver.com username=myusername password=myspassword path=/store/{fn}
```

The parameters are:

- **input** - the file to upload (optional - defaults to {tempfn}).
- **ssl** - none, ftps, ftpes, implicit, explicit - type of SSL encryption to use. **ftps** and **implicit** are identical and indicate that FTP is performed on a different port from normal (usually 990). **ftpes** and **explicit** are identical and indicate that FTP is performed on the normal FTP port, and the connection is explicitly switched to encrypted once the connection has started. (optional - defaults to none)
- **ccc** - yes or no. Indicates whether the 'CCC' (Clear Command Channel) command is used. This makes FTP work better through firewalls, but requires support from the server. (optional - defaults to no. Only if SSL is used)
- **host** - the FTP server address/name
- **passive** - yes or no. Indicates whether passive FTP is used (optional - defaults to no)
- **modez** - yes or no. Indicates whether modez is used (on-the-fly compression). This requires server support. (optional - defaults to no)
- **username** - the username to log on to the FTP server
- **password** - the password to use to log on to the FTP server

- **path** - the path to store the uploaded file
- **compression** - the level of compression (0 = less compression, quicker, 9 = more compression, slower) (optional - zip & gzip types only)
- **checkcert** - yes or no. Indicates whether to check the FTP server certificate matches the server name (optional - defaults to no. Only if SSL is used)
- **port** - the FTP port to use (optional, defaults to 21)

If you are not sure about these, you should contact the FTP server administrator who should be able to help.

SFTP

Upload a file using SFTP.

The syntax is:

```
sftp: [input=<name>] host=<hostname> username=<username> password=<password> path=<target path>
```

For instance, to sftp the filename in the variable **{compfile}** to the server **mysshserver.com** with VPOP3's target filename you could use

```
sftp:input=compfile host=mysshserver.com username=myusername password=mypassword path=/store/{fn
```

The parameters are:

- **input** - the file to upload (optional - defaults to {tempfn}).
- **host** - the SSH/SFTP server address/name
- **username** - the username to log on to the SSH/SFTP server
- **password** - the password to use to log on to the SSH/SFTP server
- **path** - the path to store the uploaded file
- **serverkeyfingerprints** - the SSH server finger print to allow (optional - defaults to allow any)
- **port** - the SFTP port to use (optional, defaults to 22)

If you are not sure about these, you should contact the SSH/SFTP server administrator who should be able to help.

5.6.13.2 Search

To get to this page, go to Settings → [Message Archiving](#) → Search

The screenshot displays the 'Mail Archiving' search interface. The search criteria are as follows:

- Sender email address: simon
- Subject: (empty)
- Recipient: (empty)
- Date: 2015-12-01 and 2015-12-30
- Attachments: (empty)
- Message Content: (empty)

The search results table is shown below:

Description	Progress	Result
from(simon) since(2015-12-01) before(2015-12-30)	100%	44

This page lets you search the VPOP3 message archive.

You can enter the data you want to search for in the boxes in the top portion of the screen - eg **Sender email address**, **Subject**, etc. Press **Start New Search** to start a new search. Note that if you search for message content, then that will take a long time, and cannot search messages which have been moved into ZIP files because VPOP3 has to access the archived messages themselves. The other search fields can be searched from an index database so will be a lot quicker. If you have to search message contents, then we recommend using other search criteria as well, such as date or sender, so that the number of messages VPOP3 has to search through for the content is reduced significantly.

The search fields are all treated as substring searches, so in the screenshot above, VPOP3 will search for 'simon' in any part of the sender's email address.

VPOP3 will find up to 1000 matching messages for each search.

VPOP3 can perform multiple archive searches at once (up to 8 per session), and will keep track of up to 8 previous searches (8 active & previous searches in total). If you need to perform more searches, you can click **Close Previous Searches** to make VPOP3 forget previous searches. The searches will also be forgotten if you log out (or the session times out).

When a search is completed the description can be clicked on to view the search results on the Results tab.

5.6.13.3 Results

To get to this page, go to Settings → [Message Archiving](#) → Search, search for messages, then click on the search results to go to the Results tab

The screenshot displays the 'Mail Archiving' interface with the 'Search Results' tab selected. The search criteria is 'test'. The results list shows the following data:

Date	Sender	Recipients	Subject	Size
29/09/2016 08:12	m...	eb sales@pscsc.co.uk	Re: Invoice from Paul Smith Computer Services	9.7kB
29/09/2016 08:13	support	r...	b [#S...]: Re: Invoice from Paul Smith Computer Services	8.7kB
29/09/2016 17:19	c...	c...	Copy of invoice	187kB
29/09/2016 17:46	l...	c...	RE: from Paul Smith Computer Services	17.3kB
08:42	cheryl	k...	Re: Invoice from Paul Smith Computer Services	17.3kB

This page shows the results of an [archive search](#). Up to 1000 results are displayed. You can select messages (use shift-click & ctrl-click to select multiple messages) and copy them to a VPOP3 user using the **Copy Messages To** option above the results list.

If you double-click on a message in the results list then you will be shown the raw message content, as well as some extra information, such as the IP address it came from (if it was received by SMTP), the authenticated sender (if any), any attachments, and so on. You will also be given a list of other messages in the same conversation (thread) which you can view. From this window you can also copy the message or entire thread to a specified user.

5.6.13.4 Offline

To get to this page, go to Settings → [Message Archiving](#) → Offline

Mail Archiving Show Hints

Use this section to move messages from the VPOP3 'Online Archive' into a disk folder for offline archiving. This can either be a folder on a removable drive, or a temporary folder on the hard disk for subsequent writing to a CD/DVD/etc

Archive Offline Backup

Archive Backup Name : 2016-09-30

Archive Backup Location : C:\vpop3

Backup Messages older than 365 days
 Backup Messages before 2015-10-01

Limit ZIP by : size number of messages

Target Backup Size : 620 MB (CD (650MB))

Allow ZIP file to be bigger than target size.
This option speeds up processing. Uncheck if ZIP will be stored on a CD/DVD/etc where a bigger file may not fit.

Use VPOP3 directory as working directory.
This option speeds up processing, but may cause issues with file permissions if archived messages are stored elsewhere.

[Start Backup](#)

The last offline archive copy failed with error code 112! (There is not enough space on the disk.)
The oldest archived message not stored in an offline archive is dated: 2006-11-29 04:05:21

Previous Offline Backups

Name	Dates	Messages Count	Messages Size
2006-04-25 (Rename)	05/08/2005-06/08/2005	21	14MB
2006-04-25a (Rename)	06/08/2005-16/08/2005	8350	702MB
2006-04-27 (Rename)	16/08/2005-06/09/2005	15181	348MB
2006-04-28 (Rename)	06/09/2005-30/09/2005	18174	264MB
2006-04-29 (Rename)	30/09/2005-18/10/2005	13098	298MB
2006-05-09 (Rename)	18/10/2005-31/10/2005	9708	249MB
2006-05-19 (Rename)	31/10/2005-17/11/2005	13609	231MB
2006-12-01 (Rename)	17/11/2005-05/05/2006	104635	1GB
2006-12-05a (Rename)	01/01/2006-19/01/2006	11529	208MB
2006-12-07 (Rename)	19/01/2006-08/03/2006	60000	750MB
2006-12-12 (Rename)	08/03/2006-15/06/2006	77027	1013MB
2012-04-24a (Rename)	13/05/2006-28/11/2006	186	8MB
2006-12-13 (Rename)	15/06/2006-16/08/2006	87661	1GB

VPOP3 Enterprise 6.20 - Imail.pscs.co.uk - 192.168.66.23 Idle In: 39326 Out: 0

This page lets you move messages out of the message archive and into a ZIP file (which can be stored elsewhere). Generally we don't recommend doing this because it makes it more complicated to search the message archive or retrieve messages from it, and disk storage is very cheap, but the option is here if you wish.

The **Archive Backup Name** is the name of the ZIP file you will create. VPOP3 puts the current date here. You cannot create two files with the same name. If an archive search finds a message which is stored in a ZIP file, this name will be displayed so you can give VPOP3 access to the correct ZIP file.

The **Archive Backup Location** is the path where the ZIP file will be stored. This must be a local folder on the VPOP3 PC.

You can tell VPOP3 which messages to backup - eg older than a certain date, or older than a certain number of days.

You can select whether to limit the ZIP file by file **size** (in MB) or the **number of messages** in the ZIP file. If you want to put the ZIP file onto a CD or DVD or other device of limited size, you should probably choose to set a maximum file size, otherwise it will be quicker if you specify a number of messages.

If you specify the final size of the ZIP file, VPOP3 cannot tell at the start how many messages it needs to put into the ZIP file because different messages will compress by different amounts, so VPOP3 will

have to create the ZIP file in several passes in this case. Because adding messages to or removing messages from the ZIP file is a very slow operation when the ZIP file is big, VPOP3 will stop the operation when it is 'close enough' rather than trying to get as close as possible and taking much longer.

If you specify the number of messages, VPOP3 will simply add that many messages to the ZIP file (assuming they are available within the allowed date range) and create a ZIP file of whatever size is needed, so it only needs to make one pass to make the ZIP file.

If you check the **Allow ZIP file to be bigger than target size** option, then VPOP3 will estimate that messages will compress at a 2:1 ratio and add enough messages into the ZIP file to make the required size if that ratio is correct. If that means that the resulting ZIP file is over the specified size, VPOP3 will stop at that point. If the ZIP file is not big enough, then it will add more messages as appropriate. This may mean that the ZIP file will be bigger than requested. In many cases this will not be a big problem and it means that the operation will be *much* quicker, but if you are going to store the ZIP file on a CD or DVD disk or something similar, then you may not want to check this option as the resulting ZIP file may not fit.

The **Use VPOP3 directory as working directory** option tells VPOP3 to store temporary files in the local VPOP3 directory. This makes the operation quicker if the archive main store is on an external drive or network share, but you may encounter permissions problems if the main store is on a network share. We suggest trying with this option checked first, and turn it off if you encounter errors related to file permissions.

Note that some other programs may not be able to read ZIP files bigger than 4GB, and if the backup is to be stored on a FAT32 drive then the ZIP file cannot be bigger than 4GB either.

Press the **Start Backup** button to start the backup process. This will often take a very long time, so you can leave this page and do other things. If you come back to this page (even after logging out and back in again), it will display the current progress, or the result of the operation. If the operation fails, then the messages will be left in the main archive store, otherwise they will be deleted from the main archive store.

At the bottom of the screen is displayed a list of all the previous ZIP files you have created, which dates are stored in it, and the number of messages and size.

5.6.13.5 Maintenance

To get to this page, go to Settings → [Message Archiving](#) → Maintenance

The screenshot displays the 'Mail Archiving' interface with the 'Maintenance' tab selected. It features a 'Request Archive Scan' button and two data sections:

Previous Rescan	
Started:	29/04/2016 10:40
Finished:	29/04/2016 22:56
Orphans Found:	0

Previous Move(s)	
Started:	25/11/2015 10:16
Finished:	25/04/2016 15:31
Move From:	\\qnap2.pscs.co.uk\vpop3archive
Started:	25/04/2016 15:31
Finished:	25/04/2016 15:33
Move From:	\\qnap2.pscs.co.uk\vpop3archive

At the bottom of the interface, the status bar shows: VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23 | Idle | In: 39328 | Out: 0

This page lets you monitor the progress of archive maintenance tasks, and trigger an archive 'rescan'

The **Request Archive Scan** button tells VPOP3 to scan the VPOP3 Main Archive store and check for message files which are in the store but not indexed in the database, VPOP3 will add these to the search index. This can be useful if the search index database is lost or cleared for some reason.

The **Previous Rescan** details show the result of the latest scan action. The 'Orphans Found' indicates how many messages were found which were not already in the index database.

The **Previous Move(s)** details show the results of recent archive moves. If you change the location of the Main Archive Store, then VPOP3 will move all the archived messages from the old store to the new one in the background, so this lets you monitor the progress of the move process.

5.6.13.6 Technical Information

Messages are stored in the archive store in raw (EML) format, with a custom header. If a forensics company needs to access the messages it should not take much effort for them to work out how to strip the custom header information.

The custom header information consists of lines with a 2 character type indicator, followed by data. Some of the header fields which may be present are:

- TY - type - POP3/SMTP - how the message was received by VPOP3
- RP - SMTP return path
- SU - subject
- IP - IP address the message came from
- TI - Timestamp in hex FILETIME format
- RC - Recipient

5.6.14 Message Authentication

Message Authentication lets you specify how VPOP3 can indicate and verify that messages are from who they say they are from.

- **DKIM/Domain Keys Tab** - these are mechanisms which sign sent messages to indicate that they have not been modified since being sent
- **Authentication-Results Tab** - this is a standard header which mail software (including VPOP3) adds to received messages to indicate the result of any authentication checks which have been performed.
- **BATV Tab** - (Bounce Address Tag Validation) is a way to confirm that bounce messages are really due to messages you sent, rather than from someone forging your email address as the sender.

5.6.14.1 Authentication Results

To get to this page, go to Settings → [Message Authentication](#) → Authentication Results

Message Authentication Settings Show Hints Submit

DKIM/Domain Keys **Authentication-Results** **BATV**

Authentication-Results header

VPOP3 will add an Authentication-Results header to the message containing the results of the DKIM validation (and SPF & Auth if the message was received using SMTP).

See [RFC 5451](#) for a description of this header

Authentication ID

The Authentication-Results header contains an Authentication ID to indicate who added the authentication header. See the RFC for a full description of this field. This field has the same format as a fully-qualified domain name. In most cases, using the server host name or domain name is a good place to start. Note that VPOP3 will remove any other Authentication-Results headers with the same Authentication ID, before adding its own (to prevent forgeries).

Authentication ID:
(leave blank to use host name specified in Misc Settings)

Gateway Servers

If messages may arrive at VPOP3 from other trusted gateway servers using SMTP, then you can specify their IP addresses below. In this case, VPOP3 will not perform the authentication checks or add the Authentication-Results header if the message arrives from one of those IP addresses, but will do so if it arrives from a different IP address

Gateway Servers:
(Separate multiple entries with spaces or semi-colons)

VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 Idle In: 40815 Out: 0

This tab is only for advanced users on complex networks. Most VPOP3 users will not need to enter any settings on this tab and can safely ignore it!

This tab allows you to set the behaviour of the **Authentication-Results** header which is defined in [RFC 5451](#). If you don't know what this header is, then you probably do not need to change any settings on this page!

The Authentication-Results header contains the results of various SMTP message authentication checks, such as SPF, DKIM and SMTP authentication. The header field has a standard format which is defined in the above RFC.

The **Authentication ID** field of the header indicates who added the authentication header. This is described in [RFC 5451 section 2.3](#). The default is that VPOP3 will use the host name specified in the [Misc Settings](#) which will be perfectly acceptable in most situations. The only time you may need to change this is if you have a system with several mail servers and you want them all to use the same Authentication ID so that other mail servers know to use the Authentication-Results header added by those mail servers.

The Gateway Servers setting tells VPOP3 not to perform authentication checks or add the Authentication-Results header if the message arrives at VPOP3 using SMTP from one of the specified IP addresses. This can be useful if messages arrive via a chain of SMTP servers; except for the "border MTA" other servers will not see the original sender IP address so cannot perform SPF checks, for instance.

5.6.14.2 BATV

To get to this page, go to Settings → [Message Authentication](#) → BATV



The screenshot shows the 'Message Authentication Settings' page in VPOP3. The left sidebar contains a navigation menu with 'Message Authentication' highlighted. The main content area is titled 'Message Authentication Settings' and has a 'Show Hints' button. Below the title is a 'Submit' button. The page is divided into three tabs: 'DKIM/Domain Keys', 'Authentication-Results', and 'BATV'. The 'BATV' tab is active. The content under the 'BATV' tab includes the heading 'BATV' and a paragraph explaining that BATV (Bounce Address Tag Validation) is a method used to check that bounce messages are in response to messages that were actually sent by you. It further explains that enabling BATV alters the return path on outgoing messages, and VPOP3 will validate that address and convert it back to the original sender. Below the text is a checkbox labeled 'Enable BATV support' which is currently unchecked. At the bottom, there is a text input field labeled 'BATV Secret:' containing the value 'abatvkey' and the text '(secret text)' below it.

BATV (Bounce Address Tag Validation) is a way of confirming that bounce messages you receive are really due to messages you sent.

It is trivial for email senders to specify any email address they wish as the address that the message came from. This means that spammers often send emails from legitimate email addresses even though they have no right to use that sender address. This will usually cause the owner of that email address to receive a storm of bounce messages from messages they didn't actually send.

BATV helps to alleviate that problem. What it does is change the *Return Path* email address on outgoing messages in a certain way (the *Return Path* address is where bounce messages are sent). Then, when bounce messages are received, the address that the bounce message is sent to can be verified to confirm that it was modified in the correct way.

The **Enable BATV support** option turns on BATV address modification and verification.

The **BATV Secret** value sets the secret value used when generating the BATV tag.

When you use BATV, if you send a message from **user@example.com**, then Return Path will be modified to something like **prvs=<tagvalue>=user@example.com**. This means that the original Return Path can easily be seen, but the **prvs=<tagvalue>** prefix indicates that it has had BATV applied to it. The value of **<tagvalue>** is calculated based on the **BATV Secret**, a timestamp and the original Return Path.

Potential problems

- BATV can sometimes cause problems if you are sending messages through an ISP which verifies sender email addresses, because the modified email addresses may not be understood by the ISP so the messages may be rejected.
- If your incoming mail is received through a third party (eg a filtering company) which checks email addresses, they may reject the bounce messages because they do not recognise the recipient. Also, this type of company may perform their own BATV checks on incoming messages, but they may not recognise the way that VPOP3 has modified the Return Path as being the correct way, so they reject the bounce messages.
- If you are sending mail through another server which performs BATV as well, then it can cause issues.

Many problems with BATV can be alleviated if the other software recognises that the address is a BATV address, so can handle it appropriately because they have a standard format so the original recipient can easily be detected.

5.6.15 Message Monitoring

To get to this page, go to Settings → Message Monitoring.

The screenshot shows the VPOP3 Enterprise 6.15 Admin Settings interface. The top navigation bar includes icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. The left sidebar contains a tree view of settings categories, with 'Message Monitoring' highlighted. The main content area is titled 'Monitoring' and features a green header bar with 'Show Hints' and 'Submit' buttons. The 'What to Monitor' section has three dropdown menus: 'Incoming messages', 'Outgoing messages', and 'Internal messages', all set to 'None'. Below this is a note: '(If Selected is chosen above, then you select which users' mail will be monitored on the Users -> Accounts -> (username) -> Permissions page)'. The 'Only monitor messages larger than' field is set to '0' KB. The 'Who receives Monitored messages' section has a 'Monitor Target' dropdown set to 'paul'. The 'Random Sample' section has a 'Send random' field set to '0' % and a 'To' dropdown set to 'paul'. The 'BCC Monitoring' section has a 'Monitor Target' dropdown set to 'No BCC Monitoring'. The 'Selected Monitored Users' section lists the following users: cheryl, Margaret, mike, and paul.

Message Monitoring lets you specify that certain messages are copied to a specified user. This can be useful for keeping track of what users are sending & receiving. Note that if you just want to keep a record of what people send/receive in case you need to look back, then the [Message Archive](#) may be more appropriate. Message Monitoring is better if you want to be informed whenever a message is sent/received, without having to check. So, for instance, Message Archiving may be a good idea for general corporate responsibility purposes, but Message Monitoring may be more useful if you have a trainee whose messages need to be checked.

Note - You should check legal restrictions before using Message Monitoring to be sure that it is allowed in your location. We are not responsible if you use this feature inappropriately. VPOP3 does not inform the original recipient/sender that the message has been monitored, but if the monitor target replies to the message (or their email client replies for them) then the original recipient/sender may discover their messages are being monitored.

You can tell VPOP3 to monitor **Incoming messages**, **Outgoing messages** and/or **Internal messages**. For each type of message, you can choose whether to monitor **All**, **Selected** or **None**. If you choose **All**, then all messages of that type will be monitored. If you choose **Selected** then messages to/from [users who have monitoring enabled](#) will be monitored. If you choose **None**, then no messages of that type will be monitored.

If you choose **Selected**, then at the bottom of the page, it lists which users' messages will be monitored.

You can also tell VPOP3 to only monitor messages over a certain size, using the **Only monitor messages larger than X kB**. This may be useful for monitoring messages which may contain attachments (or lots of copy/pasted data).

The **Monitor Target** indicates which user will receive the monitored messages. The messages that user receives will have a prefix on the subject (eg '**Mon-incoming**') and extra header fields added to indicate who the message was from or to. You can change the subject prefix by going to [VPOP3 Text Strings](#), choosing the **Monitoring** message category and altering the text in there. Note that it is possible to remove the prefix totally, but we recommend caution if doing that because it may lead to the **Monitor Target** user not realising that a message is a monitored message, and replying to it inappropriately.

You can use the **Random Sample** monitoring to monitor a sample of messages. So, you could tell VPOP3 to monitor 10% of messages to a certain user. This may be useful to let people know that messages may be monitored, but without giving the monitor target as many messages to go through. The **Random Sample** monitoring uses the same filters as the standard message monitoring. You can use both types of monitoring at the same time, to different targets, if you wish.

BCC Monitoring applies to all users, without using the specified filters. Any time a user sends a message using a BCC, a copy of that message is sent to the specified Target (unless **No BCC Monitoring** is selected). This can be useful for situations where company policy discourages using BCCs, or where there is a concern about people sending out confidential information using BCCs. (Note that in a user's settings, you can tell VPOP3 [not to allow certain users to send BCCs at all](#), as long as SMTP authentication is used. This may be more appropriate if company policy prohibits using BCCs.)

It is possible to override the basic Message Monitoring functionality using Lua Scripting if you need more complex behaviour. This requires some Lua programming knowledge so is only for advanced users.

5.6.16 Misc Settings

The Misc Settings are global settings where we couldn't think of a better section to put them.

- [General Tab](#)
- **DNS** Tab
- [Disk/memory Checking Tab](#)
- [External Fax Tab](#)
- [BATV Tab](#)
- [Proxy Tab](#)
- [Advanced Tab](#)
- **Network** Tab
- [Bandwidth Pools Tab](#)

5.6.16.1 General

To get to this page, go to Settings → Misc Settings -> General.

This page lets you set some miscellaneous settings for VPOP3.

The **Show Splash Screen at startup** option tells VPOP3 to display a splash screen when VPOP3.EXE is run directly (rather than as a service). The splash screen can be useful because it shows the startup progress.

The **VPOP3 Host Name** option tells VPOP3 what it should call itself. This is used when other computers connect to it using SMTP or when VPOP3 makes connections to other computers using SMTP. Some mail servers perform checks on this name, so, it is best to set it correctly, especially if VPOP3 is configured to send mail using [SMTP Direct](#). Ideally it should be a DNS host name which resolves to the IP address of VPOP3.

The **Automatically Update VPOP3** option is experimental and tells VPOP3 to run an automatic update program periodically to check for updates. This will not currently perform version upgrades but may install patches. The administrator will be sent an email by VPOP3 if the updater did anything.

The **Don't put deleted files into the Windows Recycle Bin** should *always* be checked. If it is not checked, then VPOP3 will delete files to the recycle bin rather than simply deleting them. This can cause excessive disk usage and pauses as Windows cleans up the recycle bin.

The **Enable Global duplicate message detection for X days** option enables a feature which compares all incoming messages against all previous messages received in the past X days. VPOP3 checks the sender, subject, date, recipients and message-id. If the message matches any previous messages it will not be distributed to any recipients who have received it previously. This detection works across all [Mail Collectors](#) & incoming SMTP.

The **Save detected Global duplicate messages in _duplicates Folder** option tells VPOP3 that if it detects a message as a duplicate using the setting above, then it will save the message in the **_duplicates** folder inside the main VPOP3 folder. This can be useful if you think the duplicate detector is

incorrectly detecting duplicates. Note that this folder is not cleaned up by VPOP3 so you should periodically check & delete messages from it to avoid it filling the disk.

The **Keep original Received: date/time on POP3 downloaded messages** makes VPOP3 copy the date/time from the latest Received: header into its own Received: header when downloading messages using POP3. Some email clients will display the Received: date/time as the time of the message rather than the sent date/time. In this case, you would see lots of messages with the same date/time of when VPOP3 downloaded the messages from the ISP. By telling it to keep the original Received: date/time, the email client will use the date/time that the message arrived at your ISP's POP3 server rather than when VPOP3 downloaded it.

The **POP3 then SMTP connection** option tells VPOP3 to first download messages then send messages. If this option is not checked then VPOP3 will perform both actions simultaneously. This option can be useful if your ISP uses the 'POP3 then SMTP' method for SMTP authentication (which is generally obsolete nowadays).

The **Anonymise VPOP3 services** option means that when someone connects to a VPOP3 service, it does not indicate that the server is VPOP3. For instance, normally if you connect to the VPOP3 POP3 service, VPOP3 will say *+OK VPOP3 Server Ready*, if this option is checked, it will say *+OK POP3 Server Ready*, so that the person connecting doesn't know which software it is. If you don't have to, we recommend leaving this option unchecked because it can be helpful during problem diagnosis to make sure you are connecting to the correct server.

The **Hide IP addresses where possible** option tells VPOP3 to hide IP address information inside *Received:* header lines. Usually VPOP3 will add a Received: header line like *Received: from 192.168.1.12 by VPOP3 (192.168.1.1)...* If this option is checked, it will add something like *Received: from user by VPOP3*. Some people like this option because it gives the appearance of improving security, but it makes problem diagnosis harder and does not significantly improve security (security through obscurity is not security).

The **Submit SMTP reputation stats to PSCS** option tells VPOP3 to periodically send anonymous SMTP reputation statistics to PSCS for analysis to improve the spam filtering. This includes things such as IP addresses which attempt to send to non-existent email addresses or send viruses etc.

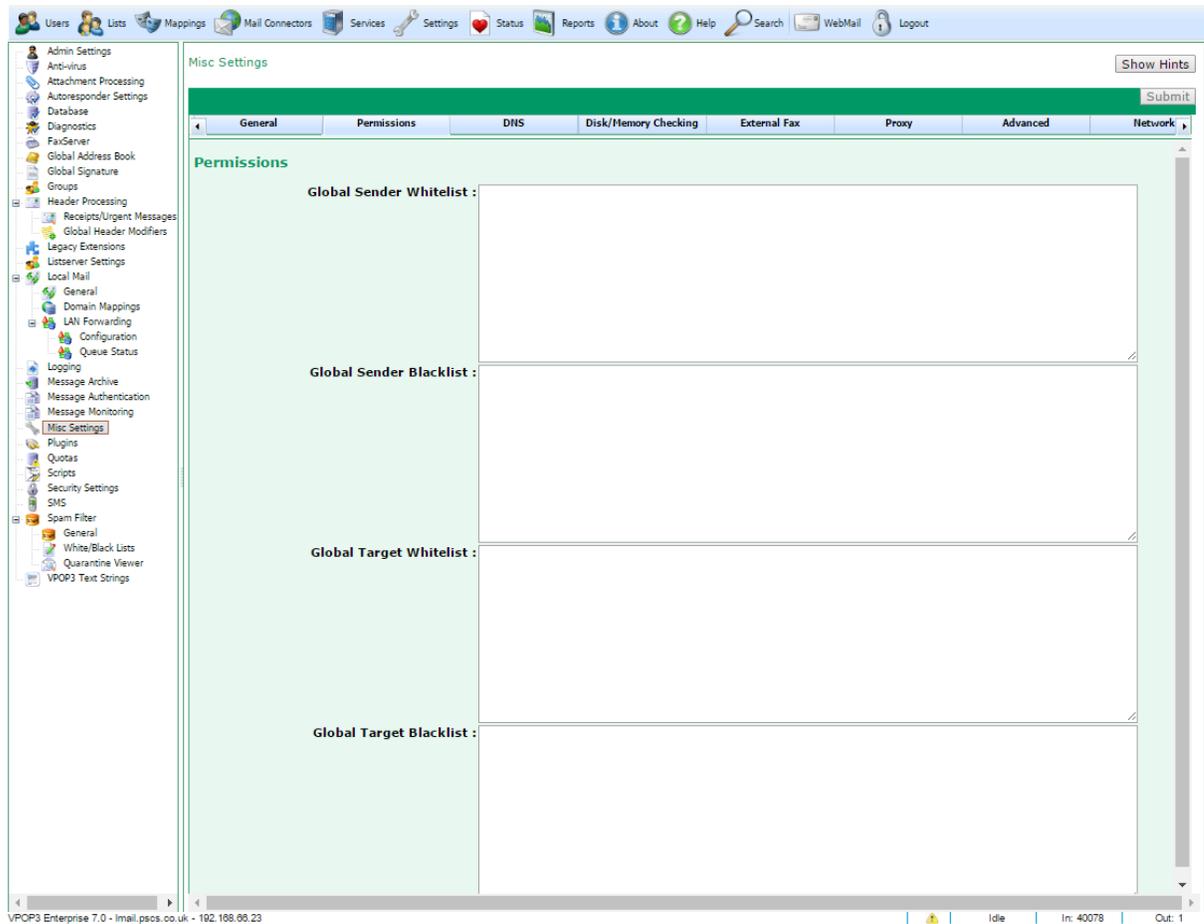
The **Include sender domain in reputation stats** option says that when sending reputation stats as above, include the sender domain (not the full email address) as well to improve the data quality.

Hold outgoing messages for ... tells VPOP3 that when someone sends a message, it should be 'held' in the Outqueue for the specified time before being allowed to be sent. This can be useful if you want to have a bit of time for senders to change their minds. The messages can be manually unheld earlier than this time if necessary. Individual users can have [different hold times](#) if desired.

Delete outgoing messages after ... tells VPOP3 that if a message is in the Outqueue for the specified time it should be deleted (the sender will receive notification that the message has been deleted). VPOP3 will usually delete messages if it has tried to send them and failed for some time - that time is set in the [Mail Sender settings](#). This option can be used in conjunction with the **Hold outgoing messages** option to implement an 'approval' system where messages which are not approved automatically get deleted.

5.6.16.2 Permissions

To get to this page, go to Settings → Misc Settings -> Permissions.



This page lets you set sender whitelist & blacklist entries for all users.

These are the same as the [sender & target whitelist & blacklist entries](#) in the user settings.

When local users send messages then the target address is checked against the user's **Target Whitelist** and **Target Blacklist** entries for that particular user, and also against the **Global Target Whitelist** and **Global Target Blacklist** on this page.

The order of processing is:

1. Is the target address on the user's target whitelist? If so, the message is allowed.
2. Is the target address on the user's target blacklist? If so, the message is not allowed.
3. Is the target address on the global target whitelist? If so, the message is allowed.
4. Is the target address on the global target blacklist? If so, the message is not allowed.
5. Are the user target whitelist and global target whitelist both empty? If so, the message is allowed
6. The message is not allowed.

Similarly, when a message is sent to a local user, the sender's address is checked against the user's **Sender Whitelist** and **Sender Blacklist** entries for that particular user, and also against the **Global Sender Whitelist** and **Global Sender Blacklist** on this page.

The order of processing is the same as for sending messages except that the sender whitelist & blacklist are checked, rather than the target whitelist & blacklist.

5.6.16.3 Disk/Memory Checking

To get to this page, go to Settings → Misc Settings -> Disk/Memory Checking.

The screenshot shows the 'Disk/Memory Checking' configuration page in the VPOP3 web interface. The page is titled 'Misc Settings' and has a 'Submit' button. The 'Disk/Memory Checking' tab is selected, showing 'Disk Space & Memory Checking' settings. Under 'Disk Space Checking', there are four settings: 'Enable disk space checking' (checked), 'SMTP Server Disk Space Check 1' (500 MB), 'SMTP Server Disk Space Check 2' (100 MB), 'POP3 Client Disk Space Check 1' (500 MB), and 'POP3 Client Disk Space Check 2' (100 MB). Under 'Free Memory Checking', there is one setting: 'POP3 Client Required Free Memory' (200 MB). The status bar at the bottom shows 'VPOP3 Enterprise 7.0 - Iml.pscs.co.uk - 192.168.66.23' and 'Idle | In: 40084 | Out: 0'.

This page lets you set how VPOP3 checks for available resources before performing some actions.

Some actions that VPOP3 performs can require a large amount of disk or memory space, so VPOP3 can check that sufficient space is available before performing these actions. The parameters for these checks are specified on this page.

Be aware that these checks are performed in regards to the resources available to VPOP3 itself, not necessarily on the whole computer that VPOP3 is running on. For instance, the disk space check is for how much space is available to VPOP3. VPOP3 checks on the disk where VPOP3 is installed, and any disk quotas on the computer will apply. So, there may be lots of free disk space, but if there is a disk quota limiting the space available to the user which VPOP3 is running as, VPOP3 may see that there is not sufficient space available to it. Also, if you are using the 32 bit version of VPOP3, VPOP3 will only have access to 3GB of RAM, regardless of how much RAM there is in the PC itself.

The **SMTP Server Disk Space Check 1** is performed before VPOP3 will accept an incoming SMTP connection. You should set this to at least 10 times the maximum size of the messages you will receive. If there is not sufficient disk space available, VPOP3 will refuse the SMTP connection and tell the sender to try again later.

The **SMTP Server Disk Space Check 2** is performed before VPOP3 will process an incoming SMTP message. You should set this to at least 5 times the maximum size of the messages you will receive. If

there is not sufficient disk space available, VPOP3 will refuse the message, and tell the sender to try again later.

The **POP3 Client Disk Space Check 1** is performed before VPOP3 will start collecting mail using POP3. You should set this to at least 10 times the maximum size of the messages you will receive. If there is not sufficient disk space available, VPOP3 will skip the POP3 collection and report an error to the administrator.

The **POP3 Client Disk Space Check 2** is performed before VPOP3 will download an incoming POP3 message. You should set this to at least 5 times the maximum size of the messages you will receive. If there is not sufficient disk space available, VPOP3 will skip the message (and try it again later) and report an error to the administrator.

The **POP3 Client Required Free Memory** check is performed before VPOP3 will start collecting mail using POP3. You should set this to at least 5 times the maximum size of the messages you will receive. If there is not memory sufficient disk space available, VPOP3 will skip the POP3 collection and report an error to the administrator.

5.6.16.4 External Fax

To get to this page, go to Settings → Misc Settings → External Fax.

The screenshot shows the VPOP3 Admin Settings interface. The top navigation bar includes icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, and Help. The left sidebar lists various settings categories, with 'Misc Settings' expanded to show 'External Fax Server'. The main content area is titled 'Misc Settings' and has a 'Show Hints' button. Below this is a 'Submit' button. The 'External Fax Server' section is active, showing a description: 'These settings are for use with an external fax server such as GFI FaxMaker™, they are not needed for the VPOP3 Fax Server.' Below the description are two settings: 'Fax Server Mailbox' with a dropdown menu set to '<None>' and an unchecked checkbox labeled 'Allow External Access to Fax Server Mailbox'. The status bar at the bottom shows 'VPOP3 Enterprise 7.0 - lmail.pscs.co.uk - 192.168.66.23' and 'Idle | In: 40983 | Out: 0'.

The External Fax settings are for use with an external email → fax software such. It helps to make it easier to use these programs; it does not provide email <-> fax services from VPOP3.

The External Fax settings simply mean that if you send an email to <faxnumber>@<your domain>, VPOP3 will send that email to the specified **Fax Server Mailbox**, rather than reporting an error because the recipient is unknown. So, if your local Domain is set to 'mycompany.com', then sending an email to 01234567890@mycompany.com or +44(1234)567890@mycompany.com will cause those messages to be sent to the **Fax Server Mailbox**.

VPOP3 recognises any otherwise unrecognised email address which contains only digits, (,), - or + in the local part as being a fax number, so it will send it to the **Fax Server Mailbox**.

If the **Allow External Access to Fax Server Mailbox** option is checked, then VPOP3 will perform this mapping rule for incoming mail as well as local mail. If this option is not checked, then incoming mail will not be delivered to the Fax Server Mailbox just because it is to a numeric local address.

5.6.16.5 Proxy

To get to this page, go to Settings → Misc Settings → Proxy.

The screenshot shows the 'Misc Settings' page with a 'Show Hints' button in the top right. Below the title bar is a 'Submit' button. A navigation bar contains tabs for 'king', 'External Fax', 'BATV', 'Proxy', and 'Advanced'. The 'Proxy' tab is selected. The main content area is titled 'HTTP Proxy Settings' and includes a descriptive paragraph: 'The HTTP Proxy is only used for HTTP connections, for instance to download spam filter or antivirus updates, etc.' Below this are two checkboxes: 'Use HTTP Proxy' (unchecked) and 'Autodetect proxy settings if possible' (unchecked). There are input fields for 'Proxy Server Address' (empty), 'Proxy Server Port' (80), 'SOCKS V4 Proxy settings' (with a sub-description: 'The SOCKS proxy is used for all connections made using a Connection method which is configured to use the SOCKS proxy.'), 'SOCKS Server Address' (192.168.57.100), 'SOCKS Server Port' (1080), and 'SOCKS Server User Name' (empty).

The Proxy settings let you configure proxy settings into VPOP3 so that it can make connections through an external proxy server. In most cases, these settings will be left blank.

VPOP3 supports the use of two types of proxy server:

HTTP Proxy

A HTTP proxy can only be used by VPOP3 to proxy HTTP connections - eg spamfilter updates, etc. Other connections, such as POP3 or SMTP connections can not be made through an HTTP proxy server.

To tell VPOP3 to use an HTTP proxy, check the **Use HTTP Proxy** box.

The **Autodetect proxy settings if possible** uses the Windows proxy detection system (the same as Internet Explorer, for instance) to attempt to detect the proxy settings automatically.

If this doesn't work, or you want to use an alternative HTTP proxy, then you can specify the proxy server address (IP address or host name) and port number in the **Proxy Server Address** and **Proxy Server Port** boxes. There is no standard for the server port, but it is often set to 80, 8000 or 8080.

Note: the **Autodetect** setting may not work if VPOP3 is running as a service. This is because the proxy detection in Windows is done on a per-user basis, and the VPOP3 service runs in a different user account from the current user. This means that it is going to be more reliable if you can manually specify the proxy server details.

SOCKS V4 Proxy

A [SOCKS v4 proxy](#) can be used by VPOP3 to proxy any type of connections, including POP3, SMTP, HTTP connections, etc.

To tell VPOP3 to use a SOCKS proxy, you need to specify the SOCKS proxy address in the **SOCKS Server Address** box, and the proxy port in the **SOCKS Server Port** box. The standard port for **SOCKS v4** connections is port 1080.

SOCKS v4 authentication uses a 'user name' only (this may be a shared secret, rather than a potentially obvious username). This is optional. Contact the administrator of the SOCKS proxy server if you are unsure what to enter here.

Note: SOCKS v5 is not compatible with SOCKS v4, so if you have a SOCKS v5 proxy server, VPOP3's SOCKS v4 support will not work with it.

5.6.16.6 Advanced

To get to this page, go to Settings → Misc Settings → Advanced.

The screenshot shows the VPOP3 Enterprise 6.20 Admin Settings interface. The top navigation bar includes: Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, and Search. The left sidebar lists various settings categories, with 'Misc Settings' selected. The main content area is titled 'Misc Settings' and contains a 'Submit' button. Below this, there are tabs for 'Disk/Memory Checking', 'External Fax', 'Proxy', and 'Advanced'. The 'Advanced Settings' section is active and displays a warning: 'It is not recommended to change these settings unless it has been suggested by a VPOP3 technical support engineer. Inappropriate changes may stop things working!'. A 'Restore Defaults' button is present. The settings include: 'Don't multi-thread VPOP3 Plugins' (checkbox), 'Max Hops' (dropdown set to 20), 'Use Fastest POP3 Download method (not recommended)' (checkbox), 'Mailer Daemon Name' (text input: Mailer_Daemon), 'Report bad mailer_daemon messages to administrator' (checkbox), 'Don't route local mail locally (use with extreme caution)' (checkbox), 'Hold Obsolete UIDs for' (dropdown set to 0 days), 'Query Download Delay' (dropdown set to 14 days), 'Use From: header address in SMTP envelope' (checkbox), 'Allow Any Line Endings' (checkbox), and 'NULL characters in POP3 downloads' (dropdown set to 'Replace with SPACE character'). The status bar at the bottom shows: VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23 | Idle | In: 40976 | Out: 1

You will normally not need to change any settings on this page unless VPOP3 technical support have suggested it.

If you do make changes, and want to go back to the original settings, the **Restore Defaults** button will restore the settings to their defaults.

The **Don't multi-thread VPOP3 plugins** option tells VPOP3 only to call plugins once at a time. If you have any VPOP3 plugins installed, then VPOP3 will usually access them as necessary, possibly with multiple processing threads at once. Correctly written plugins should be able to cope with this, however, in case you are using a plugin which crashes if it is multithreaded, you can check this box.

The **Max Hops** setting tells VPOP3 the maximum number of "hops" to be allowed when checking a new message. If the number of hops ('Received:' header lines) exceeds this number, then VPOP3 will reject the message with a 'Too many hops' error message.

In email, a 'hop' is when a message is passed from one mail server to another. When a message is received, most mail servers will count the 'hops' which a message has already made (done by counting the number of 'Received:' header lines). If this number of hops exceeds a specified value, the message will be rejected. This is because it suggests that the message may have got stuck in a loop somewhere - eg if a mail server is misconfigured, a message may be sent back and forth between two mail servers. Without the 'max hops' check, the message would go back and forth forever.

Values of 20 or higher are usually sufficient, but in a few cases, eg if all your mail passes through many mail servers (spam filtering services, archiving services etc) on the way to you, you may wish to increase this number. Do not increase it too high, or you will unnecessarily waste resources if something is misconfigured. Sensible values are between about 20 and 100.

The **Use Fastest POP3 Download method** option tells VPOP3 not to download a list of message sizes when downloading messages from a POP3 server. Usually one of the things VPOP3 does is to retrieve a list of message sizes from the remote server (using the POP3 LIST command). This is so that maximum size checks will work, and so that progress bars can be scaled appropriately. If you check this option, then VPOP3 skips this step, and assumes that each message is an arbitrary size. Nowadays, the time saved by skipping this step is negligible - eg if there are 1000 messages on the ISP, this step should take much less than 1 second, but in the days of slow modems, or if the ISP's POP3 server was not very fast, this option could be useful.

The **Mailer Daemon Name** option lets you change the name of the VPOP3 'Mailer Daemon'. In computer terms, a 'daemon' is an automated process. VPOP3's 'Mailer Daemon' is the entity which will send you emails from VPOP3 - such as error messages or other notification messages. Usually these messages will come from `mailer_daemon@<your domain>`.

Some people have wanted to change this name for various reasons, so the option to change it is here. Be aware that if you change the name, it may make technical support harder, unless you notify the support technicians of the change, as they won't be expecting the new name you have used.

Also, VPOP3 can process some control messages if you send messages with a particular format to the 'mailer daemon' address.

The **Report bad mailer_daemon messages to administrator** option tells VPOP3 to tell the VPOP3 administrator if someone sends an invalid message to the mailer_daemon. Because the VPOP3 'mailer

daemon' (see above) will send users emails, it's not unknown for some users to reply to these messages for some reason. Also, people can incorrectly format control messages to the mailer daemon.

VPOP3 will reply to the sender telling them it did not understand the message in these cases. If you check this option, then VPOP3 will also inform the administrator in case they want to use the opportunity to train the users.

The **Don't route local mail locally** option tells VPOP3 not to route mail to local email addresses internally. By default, if a local user sends a message to <a local username>@<a local domain>, VPOP3 will put the message directly into the target user's local mailbox. This is usually the expected behaviour.

If you check this option, then all messages which VPOP3 receives by SMTP will be sent out to the Internet, regardless of whether they are for a local user or not. Depending on your configuration, VPOP3 may then download the messages from a remote POP3 mailbox and distribute them to the local users.

Use of this option is strongly discouraged, as it can cause strange effects and is not a standard test use-case. Things such as BCCs, mailing lists, fax, SMS, monitoring, archiving, spamfiltering, etc are all affected if you use this option.

The **Hold Obsolete UIDLs for X days** option tells VPOP3 how long to track downloaded POP3 message Unique IDs after they have disappeared.

When VPOP3 downloads messages from a remote POP3 mailbox, it keeps track of which messages it has downloaded by remembering the UIDLs (Unique ID) of the messages it has downloaded. If VPOP3 sees a UIDL which it has not seen before, then that message will be downloaded, and if it sees a UIDL which it has seen before, the message will be ignored.

Because VPOP3 has to handle situations where other software may be deleting messages from the same POP3 mailbox which VPOP3 uses, it has to handle cases where UIDLs disappear when VPOP3 has not deleted messages. Also, it is possible for the ISP to undelete messages which VPOP3 has asked to be deleted.

The **Hold Obsolete UIDLs** option tells VPOP3 how long to remember UIDLs after they seem to have disappeared.

So, if VPOP3 deletes a message on 2 April and VPOP3 remembers UIDLs for 3 more days, it will remember that message's UIDL until 5 April. If a message appears in the POP3 mailbox with that UIDL before 5 April, VPOP3 will assume that the message has been undeleted somehow, so it will not download it again.

Some ISP POP3 servers have been known to 'lose' messages for a period, and then have them reappear, so this facility in VPOP3 stops those messages from being downloaded a second time.

Most POP3 servers will never re-use message UIDLs, as this is easy to achieve, and is the safest option. In this case, the default Hold Obsolete UIDLs setting of 3 days is safe.

However, a few ISPs will re-use message UIDLs, sometimes quite quickly. For instance, it isn't unknown for a POP3 server to give the first message which arrives in a mailbox the UIDL of 1. Then, if you delete that message, the next message which arrives will be given the UIDL of 1 again. In this case, you should set the Hold Obsolete UIDLs to 0 days to try to reduce problems with messages not being downloaded. Note that it is impossible to be perfectly safe in this situation, because if VPOP3 downloads message with UIDL 1, then some other software deletes that message (so VPOP3 doesn't know it has been deleted) and a new message arrives, the next time VPOP3 connects, it will see the message with UIDL 1, and assume it is the one it has seen before, so it will not be downloaded again. This is why most POP3 servers do not re-use message UIDLs.

The **Query Download Delay** option tells VPOP3 how long to leave messages on an ISP's POP3 server if a 'Query Download Rule' is used.

If the VPOP3 [Download Rules](#) or [Maximum Message Size To Download](#) settings tell VPOP3 to ask the user whether or not to download a message, the **Query Download Delay** tells VPOP3 how long to leave the message on the ISP's POP3 server before deleting it. This gives the user chance to respond to request the message before it is deleted.

For instance, the POP3 mail collector may be configured to delete messages after 1 day, which may not be time for the user to respond if the message in question arrives at a weekend, so VPOP3 will leave those messages in the ISP mailbox for longer (default 14 days).

The **Use From: header address in SMTP envelope** option tells VPOP3 to use the value of the From: message header as the return path in the SMTP envelope. This is normally not recommended!

When a message is sent using SMTP, the sending email client will specify the sender's address in the SMTP envelope, and also, specify the sender in the From: line in the message header.

If this option is checked, then VPOP3 will take the email address from the From: header line, and use it as the sender's address in the SMTP envelope. This should not be needed, and may break some things, so usually this option is turned off.

However, in some old versions of Pegasus Mail, this option was necessary, as the SMTP envelope sender address specified would be invalid, so using the From: header address would fix problems with sending mail.

The **Allow Any Line Endings** option tells VPOP3 to accept any line endings when dealing with other email software, rather than requiring the standard CR/LF pair.

In email, all lines must strictly end with a CR/LF pair (ASCII codes 13 + 10). Any other combinations of these characters (CR, LF, or LF/CR) are not interpreted as line endings.

Usually VPOP3 will follow the standards, however, it isn't unknown for other software which VPOP3 may communicate with not to follow the standards, and to use incorrect line endings. In this case, you can check this option to tell VPOP3 to interpret any of the four possible combinations of line endings as ending a line (CR, LF, CR/LF, LF/CR).

Note that doing this can cause problems, so we recommend not enabling this option unless instructed to do so.

For instance, in emails, the message is usually terminated by the character sequence CR LF '.' CR LF. We have seen cases where a message body (usually spam or a virus) has contained the sequence CR '.' CR in the middle. By telling VPOP3 to allow any line endings unnecessarily, this would make VPOP3 assume that the message had finished when it saw the incorrect sequence. This would cause errors subsequently as the remainder of the message is received when it is not expected.

The **NULL characters in POP3 downloads** option tells VPOP3 what to do with messages it downloads using POP3 which contain invalid NULL characters.

The POP3 standard allows any character in POP3 messages, *except for* NULL characters (characters with code 0). Legitimate messages will never contain NULL characters. Unfortunately, some POP3 mail servers breach the POP3 standard and allow NULL characters to be present in messages. This option

tells VPOP3 what to do if such a message is encountered. Leaving the NULL character in place is not an option because that would then cause VPOP3 to breach the POP3 standard as well.

Note that a NULL character in a POP3 downloaded message could also indicate a corrupted mailbox on the remote POP3 server, so further actions may make problems worse.

The options are:

- Replace with SPACE character - any NULL characters are replaced with space ' ' characters
- Replace with question mark - any NULL characters are replaced with question mark '?' characters.
- Remove character - the NULL character is removed
- Skip message - the entire message is skipped
- Abort download - the download process is aborted.

Care must be used when setting this option.

If you replace or remove the NULL character this could potentially cause messages to be passed by a virus scanner earlier in the process and then be modified by VPOP3 to a slightly different message which may not have passed the virus scanner check.

Skipping the message will cause the entire message to be lost, but other messages to be downloaded OK. This will often be acceptable because messages containing NULL characters are normally unwanted messages (eg spam or virus infected messages).

Aborting the download will cause VPOP3 not to download any further messages from the remote POP3 server until the problem has been fixed. The VPOP3 administrator will receive an error message telling them that this is what happened. This is the safest option because it gives the remote ISP chance to fix any problems with corrupted mailboxes and the message can be checked manually to make sure it is unwanted before being deleted. However, this option will almost certainly require manual intervention such as logging onto the remote POP3 server using a Webmail service from the ISP.

5.6.16.7 Bandwidth Pools

To get to this page, go to Settings → [Misc Settings](#) → Bandwidth Pools.

Misc Settings Show Hints Submit

Bandwidth Pools

Bandwidth Pools are a feature of VPOP3 Enterprise which allow more options for service bandwidth control. With the basic Service bandwidth settings you can set limit the bandwidth per session. By using Bandwidth Pools you can set a group of sessions to share a bandwidth allowance. There are 1000 Bandwidth Pools available.

Also in VPOP3 Enterprise you can have a script to set the bandwidth limit or Bandwidth Pool to use for any particular session, based on client IP address, logged in user, etc.

ID	Name	Allowed Bandwidth
1	IMAP4	-3
2	POP3	-3
3	VPOP3	100000
4	pool-4	0
5	pool-5	0
6	pool-6	0
7	pool-7	0
8	pool-8	0
9	pool-9	0
10	pool-10	0

VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 | Idle | In: 39603 | Out: 0

Bandwidth pools are a [VPOP3 Enterprise](#) feature which allow you to limit bandwidth usage more flexibly than the basic system in older versions of VPOP3 or in [VPOP3 Basic](#).

With basic bandwidth limiting, in a Service's settings you can set a throughput limit per session - eg 10kB per second per session. With this limiting, it is difficult to limit the total bandwidth usage of VPOP3, because each session has its own limit.

With Bandwidth pools, you set how much bandwidth is available in a 'pool', eg 100kB per second, and then assign sessions to that pool. All the sessions assigned to that pool will share the assigned bandwidth amongst themselves, so as more sessions are started, the available bandwidth per session reduces.

See the [Services → Bandwidth Throttling](#) topic for more details.

5.6.17 Quotas

To get to this page, go to Settings → Quotas

User Quota Settings Show Hints

Mailbox Size Quotas

This page configures how VPOP3 will handle user mailbox size quotas which are set in user's individual settings

At : 80 % of quota warn user warn administrator

At : 100 % of quota warn user warn administrator

At : 120 % of quota warn user warn administrator

Block users from sending emails at : 125 % of quota (set to 0 to disable this feature)

Daily Warnings

Every day VPOP3 can send a warning to users and/or administrators about users whose mailboxes are at a specified percentage of their mailbox quota size. (These warning messages will also be sent whenever VPOP3 is restarted).

Warn user at : 80 % of quota

Warn administrator at : 100 % of quota

Sending Quotas

By default, allow an extra: 0 % of send quota before blocking mail

VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 | Idle | In: 44805 | Out: 1

This page lets you configure how VPOP3 handles quotas.

Individual user quotas are configured in the user's setting's Quotas tab, not here.

Mailbox Size Quotas

Mailbox size quotas set a limit on how big a user's mailbox may be. This can be useful if disk space is limited or you have users who do not manage their mailboxes very well.

In VPOP3 mailbox size quotas do *not* block incoming mail as they do on some systems. This is to prevent important messages from being lost. Instead users and administrators will be warned that the mailboxes are large, and you can optionally tell VPOP3 to prevent the user from sending outgoing mail (as an extra 'encouragement' for them to delete some messages).

You can configure warnings at three stages of mailbox growth. In the above screenshot:

- When the mailbox grows above 80% of the configured quota size, the user will be sent an email telling them of this.

- When the mailbox grows above 100% of the configured quota size, the user and administrator will be sent an email telling them.
- When the mailbox grows above 120% of the configured quota size, the user and administrator will be sent a further email.

Then, you can tell VPOP3 to block the user from sending messages at a certain size. In the above screenshot the user can't send messages if their mailbox grows above 125% of the configured size. If you want to disable this feature, set this option to '0'.

As well as the warnings when a message grows over a certain size, you can also tell it to send a daily message if the mailbox is still over that size. You can set the trigger sizes separately for users and the administrator.

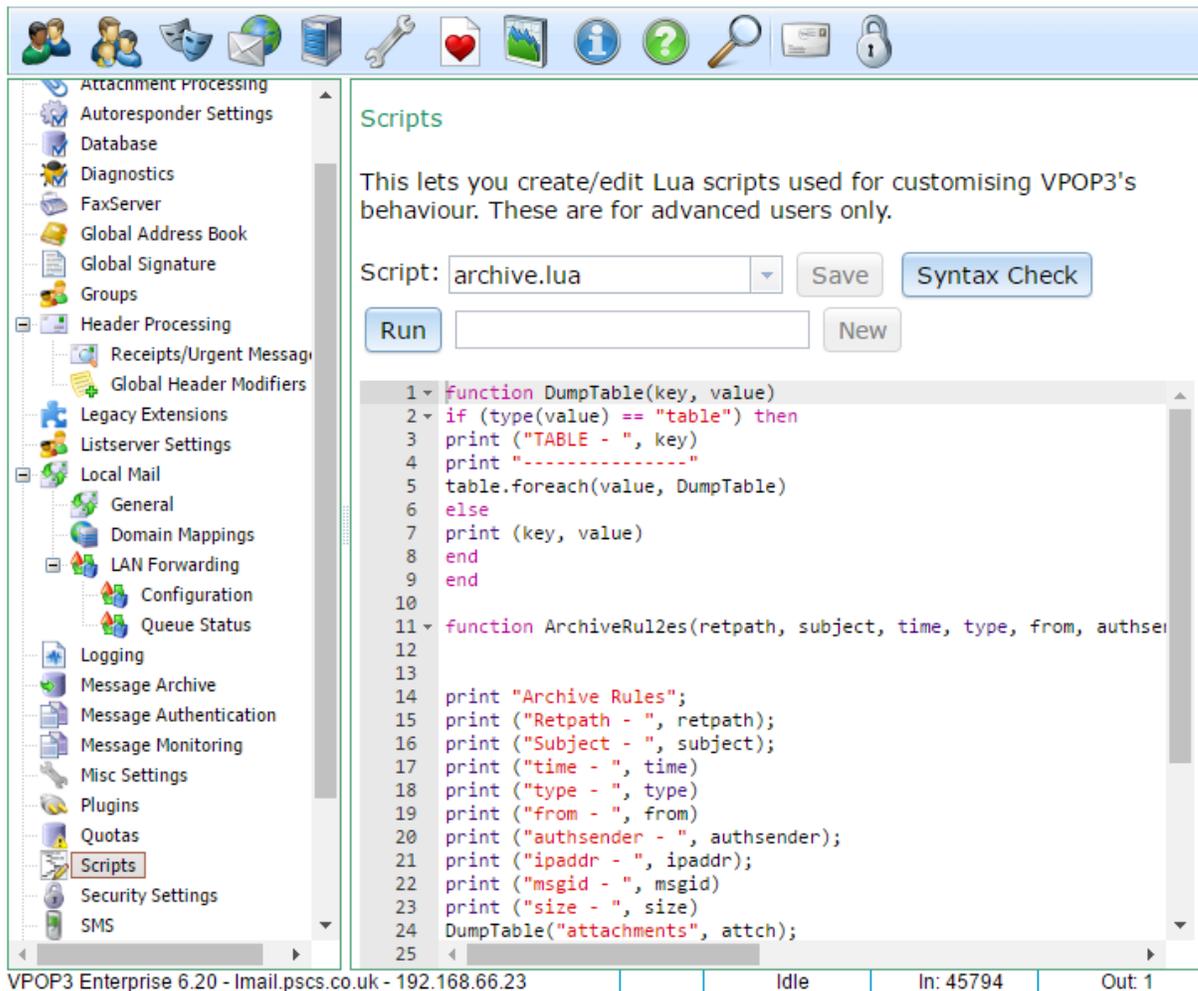
NB - the administrator who will receive the warnings is the administrator who is selected in the **MailboxQuota** target on the [Message Targets](#) list. This defaults to the [Main Administrator](#).

Sending Quotas

Sending quotas let you specify how many messages a user can send in a specified period. On this page you can specify an extra allowance on any configured quotas. (This is normally not needed as you can simply increase the user's sending quota, but the feature was requested, so it's here).

5.6.18 Scripts

To get to this page, go to Settings → Scripts



The screenshot shows the VPOP3 Admin Settings interface. The sidebar on the left lists various settings categories, with 'Scripts' highlighted. The main content area is titled 'Scripts' and contains the following text: 'This lets you create/edit Lua scripts used for customising VPOP3's behaviour. These are for advanced users only.' Below this text is a 'Script:' dropdown menu with 'archive.lua' selected, and buttons for 'Save', 'Syntax Check', 'Run', and 'New'. A code editor displays the following Lua code:

```
1 function DumpTable(key, value)
2 if (type(value) == "table") then
3 print ("TABLE - ", key)
4 print "-----"
5 table.foreach(value, DumpTable)
6 else
7 print (key, value)
8 end
9 end
10
11 function ArchiveRules(retpath, subject, time, type, from, authsender, ipaddr, msgid, size)
12
13
14 print "Archive Rules";
15 print ("Retpath - ", retpath);
16 print ("Subject - ", subject);
17 print ("time - ", time)
18 print ("type - ", type)
19 print ("from - ", from)
20 print ("authsender - ", authsender);
21 print ("ipaddr - ", ipaddr);
22 print ("msgid - ", msgid)
23 print ("size - ", size)
24 DumpTable("attachments", attach);
25
```

At the bottom of the interface, the status bar shows: 'VPOP3 Enterprise 6.20 - lmail.pcs.co.uk - 192.168.66.23 | Idle | In: 45794 | Out: 1'

This page lets you create [Lua scripts](#) which VPOP3 uses to customise behaviour. These are intended for advanced users who want to customise behaviour beyond what VPOP3 will normally do. We have decided to implement some complex features this way because the vast majority of VPOP3 users will not need those features, so adding settings to achieve them will complicate things for most users.

Lua is a programming language, so creating these scripts does need some programming ability. The [Lua website](#) has considerable documentation on the Lua language in general; the [reference section](#) of this manual, and [our Wiki](#) have more information on the specific callback functions used by VPOP3.

Lua is an interpreted scripting language designed for embedding in other software (such as VPOP3). It is commonly used as the scripting engine in games and some game mods are written in Lua.

On this page, select the script you want to create or edit from the **Script** drop-down box. After editing it, press **Save** to save it. You can press **Syntax Check** to perform a syntax check (this does not indicate that the script is correct, just that it is valid Lua).

The editor is aware of Lua syntax and performs syntax highlighting to help with your programming.

You can run the selected Lua script by pressing the **Run** button. The 'print' output will be displayed above the script. This can be useful

If you need to create a Lua script that is not in the drop-down box, then you can enter the name in the box to the right of the **Run** and press the **New** button. These extra scripts can be included in the standard scripts if you want to use the same code in several places.

5.6.19 Security Settings

The Security Settings are global settings telling VPOP3 how to handle passwords, and login attempts.

➤ [General Tab](#)

➤ [Intrusion Protection Tab](#)

5.6.19.1 General

To get to this page, go to Settings → Security Settings -> General.

The screenshot shows the 'Security Settings' interface with the 'General' tab selected. The 'General Settings' section includes:

- Minimum password length :** 3 characters
- Account Lockout Policy**
 - Lock user after :** 3 invalid login attempts
 - Lock user for :** 30 minutes
 - Apply account lockout policy to WebMail/Admin even when connecting from 127.0.0.1.** (Caution - turning this option on may make the settings temporarily inaccessible if you forget the administrator password!)
- Windows Password Integration**
 - Allow users to log in using their Windows Passwords** (This is only possible if the users' passwords are sent to VPOP3 in unencrypted form)
 - Cache Windows Passwords** (improves performance but can affect Windows security)

Buttons for 'Show Hints' and 'Submit' are visible at the top right of the form.

The **Minimum Password Length** option sets the length (in characters) of the shortest password which can be set. This only applies to passwords set after this setting has been changed.

Account Lockout Policy

If someone tries to log into an account and specifies an incorrect password several times in a row, then VPOP3 will lock access to the account from that IP address for a short time. This is to make password attacks harder. The user will not be told that the account has been locked; they will just be told that the login failed, even if they enter the correct username & password.

VPOP3 will only lock access from the IP address which had the failed login attempts. This is to prevent someone deliberately failing login attempts to cause a denial-of-service (DoS) attack.

You can tell if an account is locked because the [Users list](#) will display a padlock icon to the left of the account name. You can unlock an account by editing the account, and clearing the **Account Locked** checkbox on the [User's General tab](#).

The **Lock user after x invalid login attempts** setting tells VPOP3 how many failed login attempts are allowed before the account is locked.

The **Lock user for x minutes** setting tells VPOP3 how long to lock the account for once the allowed failed login attempts has been exceeded. Once this time is up, then the account will automatically unlock itself.



Tip

If the administrator account is locked, and you cannot wait the specified time for the account to unlock, then you can restart the VPOP3 service to force all the account locks to be removed.

You can also try accessing the VPOP3 settings from the VPOP3 PC itself (see below).

Normally, VPOP3 will not lock out accounts if they are accessed from the TCP/IP loopback address (127.0.0.1). This is to always allow administrator login from the VPOP3 computer itself. This assumes that the VPOP3 PC is physically secured so that hackers cannot gain access to it, and also cannot gain access via remote-desktop or other remote control software. The **Start » Programs » VPOP3 » Configure VPOP3** link in the Windows menus will access the VPOP3 settings using the loopback address.

If you wish VPOP3 to apply the lockout policy to the loopback address as well, you can check the **Apply account lockout policy to WebMail/Admin even when connecting from 127.0.0.1** option. However, note that doing so may make it much harder for a legitimate administrator to gain access to VPOP3's settings if they are unsure of the login password.

Windows Password Integration

VPOP3 has its own user database system. It is not linked into a Windows user database such as Active Directory. This is for several reasons. For instance:

- ❖ VPOP3 will run on any version of Windows, not just Windows Server versions. If VPOP3 required the Windows user database, then installation on desktop versions of Windows could be troublesome.
- ❖ Some email authentication methods would not be available if VPOP3 only used the Windows user database because of how Windows allows third party programs to access the user database.
- ❖ Many times users do not want the email passwords to be linked to their Windows passwords. Often email passwords are configured into an email client and are not changed, but Windows passwords may expire regularly.

However, VPOP3 has some features which may help with installations where people want to be able to use Windows login details to access VPOP3. To use these features, VPOP3 needs to know the Windows username relating to the VPOP3 username. In the simplest case, the VPOP3 usernames and Windows usernames will be identical. If that isn't the case, then the administrator can set the Windows username for a VPOP3 user in the [user's Advanced tab](#).

If the **Allow users to log in using their Windows passwords** option is checked, then VPOP3 will allow users to log in using either their VPOP3 login details, or their Windows passwords. Note that VPOP3 can only check passwords against the Windows user database if VPOP3 receives them in plain text. Hashed passwords, such as CRAM-MD5 passwords cannot be checked against the Windows user database. To avoid sending Windows passwords in plain text across the network you should consider using [session encryption](#) (requires [VPOP3 Enterprise](#)).

If the **Cache Windows passwords** option is checked, then, if VPOP3 detects that a user has entered their Windows password, VPOP3 will update its own user database to match the same password that the user entered. This will invalidate the previous VPOP3 password. We do *not* recommend the use of this option because the encryption method which VPOP3 uses for storing the passwords may not be as secure as the method which Windows uses, meaning that storing the passwords in a possibly less secure database may compromise security.

5.6.19.2 Intrusion Protection

To get to this page, go to Settings → Security Settings -> Intrusion Protection.

The screenshot shows the 'Security Settings' interface with the 'Intrusion Protection' tab selected. The 'Intrusion Prevention' section is active, displaying the following settings:

- Monitor logins period :** 30 minutes
- Failed login threshold :** 10
- Failed login block time :** 30 minutes

At the bottom of the settings area, there are three buttons: 'Manage Block List', 'Manage Never Block List', and 'View Event Log'. A 'Submit' button is located at the top right of the settings area.

The **Intrusion Protection** tab offers settings which expand on the normal **Account Lockout** policies (see above). The Account Lockout policies treat each user account as a separate entity - so someone could try to log into 300 different accounts once each, and not be locked out, because VPOP3 only counts consecutive failed logins for each account separately.

The **Intrusion Protection** feature will count failed login attempts by the user's IP address. So, if someone tries to log into 10 different accounts (whether or not they actually exist in VPOP3) within 30 minutes, then VPOP3 will block access from that IP address for 30 minutes (assuming the settings in the screenshot).

The **Monitor logins period** tells VPOP3 how long it should monitor login attempts over. If this is set to 30 minutes, then a failed login attempt that was made 31 minutes ago is not counted.

The **Failed login threshold** tells VPOP3 at what point it should block an IP address. So, if this is set to 10, then when the 10th failed login attempt is made from an IP address, that IP address will be blocked.

The **Failed login block time** tells VPOP3 how long it should block a suspicious IP address for.

VPOP3 will add blocked IP addresses into a **Block List** and it will check a **Never Block List** before blocking an address, so that those IP addresses are never blocked. This facility uses the same **Block** and **Never Block** lists that the [SMTP IPS system](#) uses

The **Manage Block List** button shows a window containing the IP addresses which are currently blocked, and telling you when they were blocked, and when the block expires. If you double-click on an address, it will tell you why that address was blocked. You can select an address and press the **Delete** button to remove the address from the list. You can manually add entries to the Block List by typing them in the **Address** box at the bottom of the window, entering the time to block the message for into the **Period** box, and pressing the **Add** button. You cannot block an address for ever, but you could enter **99999999** minutes into the Period to block the address for nearly 200 years. The **Address** you enter can be in [CIDR format](#), eg `123.123.123.0/24`.

The **Manage Never Block List** button shows a window containing the IP addresses which VPOP3 is never to block. These would usually be internal or trusted IP addresses. You can select an address and press the **Delete** button to remove the address from the list. You can manually add entries to the Never Block List by typing them in the **Address** box at the bottom of the window, and pressing the **Add** button. The **Address** you enter can be in [CIDR format](#), eg `192.168.1.0/24`.

The **View Event Log** button will show a window containing the most recent failed login attempts, and where they are coming from. If your VPOP3 is accessible from the Internet (to allow remote access) it is not uncommon for there to be lots of failed login attempts here (especially from spammers attempting SMTP logins). Generally it is not worth getting too worried about as long as your users' passwords are relatively secure.

5.6.20 Spam Filter

The Spam Filter settings relate to the VPOP3 spam filter & content filter.

This is a script/rule based system for content filtering messages. Usually it is used as a spam filter, but it can be used to perform many different content filtering tasks as well.

- [General Settings](#) - configure the behaviour of the spam/content filter
- [White/Black Lists](#) - configure email address & word whitelists and blacklists for the default spam filter behaviour
- [Quarantine Viewer](#) - view & release messages which are quarantined by the spam filter

5.6.20.1 General

The Spamfilter → General Settings are where you configure the behaviour of the VPOP3 spam/content filter.

- [General Tab](#)
- [Quarantine Settings Tab](#)
- [Bayesian Database Tab](#)
- [Script Configuration Tab](#)
- [Rule Weights Tab](#)
- [Advanced Tab](#)

5.6.20.1.1 General

To get to this page, go to Settings → [Spam Filter](#) → [General](#) → General.

This page lets you configure the VPOP3 Spam filter and view some information about it.

The **Enable Spam/Content filter on SMTP messages** option tells VPOP3 whether to pass messages it receives using SMTP through the spam filter. This includes internal and incoming SMTP messages. The spam filter knows when a message is sent from a trusted IP address or authenticated user. If so, it does not test to see if the message is spam, instead it trains the [Bayesian spam filter](#) that this is a 'good' message, and optionally adds the recipient(s) into the [spam filter whitelist](#) so that any replies will be allowed through the spam filter.

The **Enable Spam/Content filter on POP3 messages** option tells VPOP3 whether to pass messages it downloads using POP3 through the spam filter. This will only include incoming messages.

The **Timeout** options tell VPOP3 how long the spam filter should run before it gives up. For incoming SMTP, if it times out it will send a 'temporary reject' response to the sender which will tell them to try again later. For incoming POP3, the message will be handled as if not spam. Generally, on a well specified server the filter should take no more than a few seconds - most of this time will be waiting for DNS responses.

The **Automatically download spam filter updates** option should be turned on if you have a subscription to our spam filter updates. If you don't have a subscription, then you can still use the spam filter, but you will not receive updates to handle the latest spam, so it will be less effective. You can update the spam filter yourself if you wish - the [script language definition](#) is available on our website to help you.

If the updates are turned on, then beneath that option is status information showing when VPOP3 last checked for updates, last downloaded updates, when your subscription expires, etc.

The **Report successful spam filter updates to administrator** option tells VPOP3 to tell the administrator when it has downloaded an update successfully. VPOP3 will always tell the administrator if it has failed to check for updates successfully for an extended period of time.

The spam filter uses DNS servers for accessing real-time databases to help with spam filtering, such as blacklists, whitelists etc. The **DNS Test Results** section shows the access times for retrieving existing and non-existent DNS results. If these are too high, then it may suggest a problem with the DNS server which VPOP3 is using. That may lead to less accurate filter results, or slow performance.

5.6.20.1.2 Quarantine Settings

To get to this page, go to Settings → [Spam Filter](#) → [General](#) → Quarantine Settings.

Spam/Content Filter Show Hints

Changes have been made - press:

General | **Quarantine Settings** | Bayesian Database | Script Configuration | Rule Weights | Advanced

Quarantine Settings

Enable Quarantine facility

Delete messages from the Quarantine after : days

Quarantine Server Address : (this is the VPOP3 server address as the users see it to access WebMail. eg if they would go to http://192.168.0.1:5108 to access the VPOP3 WebMail, set this to **192.168.0.1**)

Each user can have their own level at which mail will be quarantined rather than delivered to the user. You can set these on each user's **Advanced** settings page individually. Alternatively, you can set it for all users by entering a non-zero value below. (Users' individual settings will override this value if set)

Default Quarantine Threshold :

Clear all users' individual quarantine thresholds

Allow viewing of quarantined messages without logging in (or when logged in as a different user)

Quarantine Daily Reports

In the quarantine viewer and the emailed daily reports there are three levels of colour which can be applied to the messages to indicate the level of spam 'score' which VPOP3 has assigned to the message.

Level 1 :

Level 2 :

Level 3 :

Send all quarantine reports to : (leave blank to send to original user)

Sort Quarantine reports by :

Quarantine Report Schedule :

Generate quarantine report now for :

The Quarantine Settings let you tell VPOP3 when to put messages into the [spamfilter quarantine](#), how long to leave them there, and how to send daily quarantine summaries to the users.

The **Enable Quarantine Facility** box lets you globally enable/disable the quarantine facility. If it is disabled, then no messages will be put into the quarantine. If it is enabled, then messages which are determined to be spam will be quarantined. Note that, if the quarantine is enabled, you can selectively [configure VPOP3 not to quarantine specified users' spam messages](#) if you wish.

The **Delete messages from the quarantine after ... days** setting tells VPOP3 how long messages should remain in the quarantine before being automatically deleted. We recommend that you set this to a few days longer than the maximum time people will usually be unable to access their mail. For instance, two to three weeks is usually a good starting point. If you make it too large, then the server's

hard disk will fill up with lots of probable spam messages. If you make it too small, then incorrectly quarantined messages may be deleted before the user has chance to release them from the quarantine.

The **Quarantine Server Address** setting tells VPOP3 what server address to use in the links in the daily quarantine summary report emails sent to the users. This should be an address which the users can use. In a simple setup, this would be the internal IP address or name of the computer running the VPOP3 software (VPOP3 will use the IP address in this setting during installation). However, this will not work if users can access their mail from outside the local network. If you want users to be able to access their quarantined messages from outside the local network, you probably need to configure a DNS host name which will resolve appropriately to allow access from inside and outside your local network. Then, specify that DNS host name in the **Quarantine Server Address** setting on this page.

The **Default Quarantine Threshold** tells VPOP3 when spam messages should be quarantined. Each message that is processed by the spam filter is given a score, with bigger scores meaning the message is more 'spammy'. The filter is designed that a message with a score of **100** is probably spam. So, if you set the **Quarantine Threshold** to 100 (the default) it will be put into the quarantine rather than delivered to the user. If you want to have fewer messages quarantined, but receive more spam, then you can increase this number. If you want to receive less spam (and probably have more legitimate messages quarantined) you could decrease this number. The **Default Quarantine Threshold** sets the score at which messages are quarantined unless [users have individual quarantine thresholds](#) set differently.

If you check the **Clear all users' individual quarantine thresholds** box and press the **Submit** button, then all the [users' individual quarantine thresholds](#) will be cleared, so that the **Default Quarantine Threshold** will apply to all users again.

Normally, a user needs to log into their Webmail before they can view their quarantined messages. This is for security purposes. In some cases, this may be deemed unnecessary - for instance because the Webmail service is only accessible from the local network, or users can't remember passwords, or quarantined messages are considered not to be valuable. In this case, you can check the **Allow viewing of quarantined messages without logging in** box. In this case, the links in the quarantine summary report will be accessible even if the user doesn't log in, or is already logged in as a different user. In this case, there is a risk that an unauthorised user could access quarantined messages they shouldn't be able to see, but it is not trivial to guess the links to use, and the messages are probably of low value, so you may consider this a worthwhile compromise to get more convenience.

Quarantine Daily Reports

When VPOP3 sends a daily quarantine report it colour codes the messages depending on their spam filter score. You can configure the levels of the colour changes using the **Level 1**, **Level 2** and **Level 3** options. Level 1 messages are displayed in **blue**, Level 2 messages are displayed in **red** and Level 3 messages are displayed in **dark red**. (Level 1 messages are not displayed in green, because they are not 'good' messages, just less bad than level 2 messages).

Normally, the quarantine report email messages are sent to the user whose quarantine contains the messages. If you wish, you can specify an alternate email address in the **Send all quarantine reports to** box, and VPOP3 will send all the quarantine reports to the specified address. You can specify exceptions to this using the [Daily Quarantine Report Recipient](#) setting in an individual user's settings.

The daily quarantine reports can have the quarantined messages sorted by different data as you find useful. This is set using the **Sort quarantine reports by** setting. Probably, the most useful option is to sort by the **Spam Score**, which will mean that the most likely incorrectly quarantined messages are at the top of the report.

The **Quarantine report schedule** setting lets you specify when VPOP3 will send out the quarantine reports. Usually, VPOP3 will send the messages out at midnight, but some people would prefer the messages to be sent out during the day, or would like to receive several summary messages a day. You

can specify a list of times to send out the messages in the **Quarantine report schedule** box. Simply specify the hours in 24 hour format - e.g. "9 16" will make VPOP3 send out the emails at 9am and 4pm. (You cannot specify the minutes of the times to send the emails).

The **Generate quarantine report now for** option lets you generate a quarantine report for a user using the options set on this page. It can be useful for testing the settings here, or for generating a report email if someone needs one generated before the normal scheduled time.

5.6.20.1.3 Bayesian Database

To get to this page, go to Settings → [Spam Filter](#) → [General](#) → Bayesian Database

Spam/Content Filter Show Hints Submit

Bayesian Database

The Bayesian database is a database containing statistics of how often words or header data is contained in spam or not-spam messages handled by VPOP3. The spam filter can use a statistical method called "Bayesian Analysis" to use this data to try to determine whether a new message is likely to be spam or not-spam.

Usually you will not need to manage the Bayesian database at all, because VPOP3 will automatically manage it, but if you do want to, you can choose to delete some or all items from the database using this page.

The Bayesian statistical database currently contains 1469256 terms over 122247729 messages. (Using approx 217.8MB)

Clear Bayesian Statistics

Bayesian Analysis

Enter text in the box below and press 'Analyse' to see how VPOP3's Bayesian filter would analyse this message. Be sure to enter the full message headers as well as the message source.

```
"http://info.edgewave.com/u/d10SqaELMI0TM00J79020D0" style=3D"color: #00ade=
e; text-decoration: none;"
>unsubscribe</a> at any time.<br /><br /></div>
</body>
</html>
-----_Part_-2136550796_164560003.1472569541466--
```

Final Result: 0

Word	#Ham	#Spam	%Ham	%Spam	Calc
X-Binding:ipb-sj-01	418	7	0.0	0.0	0.000393
Received:SJMTA06.MARKETO.ORG	189	4	0.0	0.0	0.000497
Received:SJMAS01.MARKETO.ORG	713	18	0.0	0.0	0.000593
DKIM-Signature:MKTRROUTE.COM	187	7	0.0	0.0	0.000879
DKIM-Signature:@MKTRROUTE.COM	187	7	0.0	0.0	0.000879
X-MktMailDKIM:true	1304	71	0.0	0.0	0.001278
DKIM-Signature:M1	2179	122	0.1	0.0	0.001314

VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 Idle In: 51465 Out: 0

The Bayesian Database is a database which is managed by VPOP3 containing statistics of previously received messages and their contents and whether they were detected as spam or not spam.

This database is used by the [Bayesian Filter](#) component of the spam filter.

After some time the database can contain details of many messages (eg the above screenshot shows that this installation contains details of over 120 million messages). This is not usually a problem.

VPOP3 will periodically maintain the database contents so that it does not grow uncontrollably - eg by removing terms which have only rarely been seen because they are unlikely to be useful.

If you wish, you can explicitly clear database entries using the **Clear Bayesian Statistics** section. You can select entries based on how many times they have been seen, and clear them. So, for instance - *'with count=1'* means that the term (word) has been seen in only one message so far.

Bayesian Analysis

The **Bayesian Analysis** section lets you perform a manual Bayesian analysis of an email message using VPOP3's Bayesian filter/database. You should copy/paste the message to analyze into the first box, and press the **Analyse** button. Make sure you include the full message headers of the message, because those are also used for the analysis.

After pressing the **Analyse** button, VPOP3 will show the Final Result value - this ranges from 0 for "definitely not spam" to 100 for "definitely spam". Below that it shows the 'terms' detected in the message, and details of the analysis of those.

The most 'interesting' terms are marked in bold - these are the only terms which are used to calculate the final result. Note that terms include message header fields as they are also indicative of the message spamminess just as the message content itself is - for instance, messages from a certain location may have a very low likelihood of being spam. Header field terms are shown as *<header name> ":" <header data word>*.

Then, the columns displayed are:

- **# Ham** - the number of times this term has been seen in 'ham' (not spam) messages.
- **# Spam** - the number of times this term has been seen in 'spam' messages.
- **% Ham** - the percentage of times this term has been seen in 'ham' messages.
- **% Spam** - the number of times this term has been seen in 'spam' messages.
- **% Calc** - the calculation of how 'spammy' this term is (low numbers are less spammy - a term which has only ever been seen in 'ham' messages will have a value of 0, and a term which has only ever been seen in 'spam' messages will have a value of 100).

See the [Bayesian Filter](#) section for more details on how the Bayesian analysis works.

5.6.20.1.4 Script Configuration

To get to this page, go to Settings → Spam Filter → General → Script Configuration.

The screenshot shows the 'Spam/Content Filter' configuration page in VPOP3. The 'Script Configuration' tab is selected, displaying the following settings:

Setting Name	Value	Description
AllowQuickEnd	1	(Allow quick spam filter end if common current spam is found (1=yes, 0=no - default=yes))
AutoWhiteList	1	(Automatically whitelist addresses which are sent to (1=yes, 0=no))
BCCRedirect		(The user to redirect detected BCC messages to (leave blank for none))
CheckLocalWhitelist	0	(Check local mail addresses against whitelist (1=yes, 0=no) - default = no)
DontRedirect		(Don't redirect if this user is a recipient (leave blank for none))
EarlyDNS	0	(Do DNS checks early - only recommended for incoming SMTP (1=yes, 0=no - default=no))
FollowURLs	1	(Follow suspicious URLs in messages to see if they are redirections (1=yes, 0=no, 2=more checks))
ForwardSpamReport	0	(Automatically forward messages sent to 'spam' to spamreport@psecs.co.uk (1=yes, 0=no))
Redirect		(The user to redirect detected spam to (leave blank for none))
RejectBounces	0	(Reject bounces/spam confirmations (1=all, 0=only if recipient is not recognised) - default = 0)
ReverseDNSChecks	1	(Number of Received headers to check for ReverseDNS addresses (1 if direct incoming SMTP, more otherwise))
SpamPrefix	VPOP3-SPAM:	(The prefix to add to detected spam (leave blank for none))

At the bottom of the page, the status bar shows: VPOP3 Enterprise 6.20 - Iml.psecs.co.uk - 192.168.66.23 | Idle | In: 45812 | Out: 0

The VPOP3 spam filter behaviour can be customised by an administrator by using various settings. Because the filter can be updated dynamically, either by downloading using a subscription, or by manual editing from the user, these script settings may change over time, so they are listed in this one location. The settings are all text strings inside VPOP3, but the script may require special values, eg '0' or '1' to be meaningful to the script. No checking is performed on the values, so if you enter an invalid value, the behaviour may not be what you expect.

To change a settings, simply enter it into the box and press the **Submit** button.

The script settings at the time of writing are listed below with descriptions. As mentioned above these may change over time, or you could add your own settings by writing custom scripts, so the list of options here is not definitive.

AllowQuickEnd

The spam filter script can take some time to process a message depending on server specification. It performs some checks at the start of the process then the rest of the checks later (eg black/whitelist checks, some current spam attack checks, etc) . If this option is set to '1' then, after the initial set of checks, if the message has been marked as spam, or definitely not spam (eg whitelisted) then the rest of the checks will be skipped. This saves time and reduces load on the server. It does mean that it is slightly more likely to generate false positives, but our tests show this likelihood is minimal.

AutoWhiteList

If this is set to '1', then when a message is sent from a local or authenticated user, any recipients of that message are added to the [spamfilter address whitelist](#). (Also see the WhiteList.... options below)

BCCRedirect

If this option is set, then any BCCd messages that are detected will be redirected to the address specified in this option. Note that detecting BCCs is not guaranteed because there is (by definition) no message header to indicate that a message has been BCCd, but it should work in the vast majority of cases.

CheckLocalWhitelist

By default, if an *incoming* message arrives from an apparently local email address, VPOP3 will NOT check it against the address whitelist. That is because in most cases, messages from local email addresses will be sent via VPOP3 either from local computers or using SMTP authentication. Spammers very often pretend to send mail from local email addresses, so incoming mail from local email addresses should usually be treated with suspicion, not allowed through as whitelisted.

In some cases, you may want to receive incoming mail from local email addresses. In that case, change this option to '1', so that VPOP3 will always check the sender against the whitelist, even if the sender appears to be a local email address.

DontRedirect

This option disables the **Redirect** option below if the user specified here is a recipient of the incoming message.

EarlyDNS

The VPOP3 spam filter performs lots of DNS queries to look up data in real-time databases of various sorts. DNS queries can take some time to complete, even up to a second or two in some cases, that will slow the spam filtering process down.

If **EarlyDNS** is set to '1', then VPOP3 will issue the DNS queries, then perform a few checks, then check the DNS query results. This increases the overall processing time for checking messages because it may have to wait for DNS results, however this waiting time does not increase server load. Then, VPOP3 may be able to use the DNS query results to decide to 'quickly end' (see **AllowQuickEnd** above) the filtering process, which will reduce overall server load.

If **EarlyDNS** is set to '0', then VPOP3 will issue the DNS queries, then perform most of the checks, then check the DNS query results. This reduces the overall processing time for checking messages because it will probably not need to wait for the DNS results. VPOP3 cannot use the DNS query results to decide to 'quickly end' the filtering process because the results are checked too late.

If you have incoming SMTP, then **EarlyDNS** should probably be set to '1' to reduce overall server load when handling multiple incoming connections. If you have incoming POP3, then you may want to set it to '0' so that messages are processed more quickly as they arrive sequentially.

FollowURLs

If this is set to '0' then VPOP3 will do nothing if it sees a URL (link) in a message. If it is set to '1', then VPOP3 will follow some links to see where they go. This can be useful if the email contains URL shorteners. The URL shortener may redirect to a known spam website, so the message can be detected as spam in this case, whereas it can't be detected as spam if the filter just sees the URL shortener address. Also, if VPOP3 downloads the link it can check the page data for spammy data (eg redirects or keywords).

The disadvantage is that there is a possibility that by following the URL, it will inform the spammer that the email address is valid. The spam filter will try to reduce this possibility by removing query data etc from the URLs, but it cannot be guaranteed.

If this is set to '2', then VPOP3 will follow more links which will increase the likelihood of spam being detected, but may increase the chance of verifying email addresses.

We recommend you use '0' or '1' here.

ForwardSpamReport

If this is set to '1', then if a user forwards a message to 'spam@<your domain>', then VPOP3 will forward a copy to us for analysis.

Redirect

If this is set, then VPOP3 will redirect any detected spam to this address. This may be used as an alternative to (or as well as) the [quarantine](#) facility - eg some people redirect spam to a user called 'spambox' which they check periodically in their email client. The disadvantage of doing that is that you need to get any false positives to the original recipient somehow, and forwarding may change reply addresses etc.

RejectBounces

If this is set to '1', then VPOP3 will treat any message which it can identify as a bounce message as spam. If it is set to '0', then VPOP3 will only treat bounce messages which are for unrecognised recipients as spam.

ReverseDNSChecks

This is a number to say how many IP addresses listed in Received: headers it should check for reverse DNS entries. For direct incoming SMTP this can (and should) be set to '1'. If your mail arrives through your ISP, then you should increase the number so that VPOP3 will check the Received: header just before it arrived at your ISP. This cannot be determined automatically by VPOP3, and will need inspection of the Received: headers to work out how many steps the message goes through at your ISP.

It will not cause any problems if this is left as '1', but it means that one particular check won't yield any useful results.

SpamPrefix

If the spam filter gives the message a higher spam score than the **SpamThreshold** (below), then it will add the **SpamPrefix** onto the start of the message subject line

SpamThreshold

This is the spam filter score threshold above which the spam filter will decide the message is spam. This is different from the [Quarantine Threshold](#). The spam filter script runs, assigns a score, and performs some actions based on this threshold (eg adding a subject prefix etc). Then, VPOP3 afterwards decide whether to quarantine the message based on the score, or deliver it, and so on. Quarantine thresholds can be different for each recipient.

UpdateBayes

If this is set to '1', then the VPOP3 spam filter will add incoming messages which are detected as spam to the 'Spam' [Bayesian data](#), or which are not detected as spam to the 'Ham' Bayesian data. If this is '0' then the Bayesian data is not updated automatically at all (but will still be updated for message sent to spam@ or notspam@ or released from quarantine).

UseURIBL

If this is set to '1' then the VPOP3 spam filter will use the URIBL.COM real-time blacklists. If it is set to '0' then it won't. This option is because URIBL have usage limits for free access, and if you go over the usage limit, they can mark all messages as spam.

WhiteListDomainBlock

For the "AutoWhiteList" option, outgoing messages have their recipients added to the whitelist. The WhiteListDomainBlock lets you specify a domain which is not to be added to the whitelist automatically.

WhiteListFromRegExpBlock

For the "AutoWhiteList" option, outgoing messages have their recipients added to the whitelist. The WhiteListFromRegExpBlock setting lets you create a [regular expression](#) to specify SENDER addresses whose recipients will not be added to the whitelist automatically. This can be useful if you have any software which replies to incoming messages automatically (eg helpdesk software or a customer relationship management system).

An example would be:

```
/(postmaster|sales|support|webmaster)@pccs.co.uk/i
```

WhiteListRegExpBlock

For the "AutoWhiteList" option, outgoing messages have their recipients added to the whitelist. The WhiteListRegExpBlock settings lets you create a regular expression to specify target addresses which are not to be added to the whitelist automatically.

5.6.20.1.5 Rule Weights

To get to this page, go to Settings → Spam Filter → General → Rule Weights.

The screenshot shows the 'Spam/Content Filter' configuration page in the VPOP3 Enterprise 6.20 web interface. The 'Rule Weights' tab is selected, showing a table of rules with adjustable weights for Bayes scores less than or equal to 90 and greater than 90. The table includes a 'Reset Default Weights' button and a 'Description' column for each rule.

Rule Name	Bayes <= 90	Bayes > 90	Description
8Bits :	0.5 (0.5)	0.5 (0.5)	successive 8 bit characters in email
Adult :	1 (1)	2 (2)	Keywords for adult/porn emails
AdultMisspelling :	1 (1)	1 (1)	Deliberate ADULT misspellings
AdultMovies :	1 (1)	1 (1)	Porn movie spam
AdultSynonyms :	1 (1)	1 (1)	Words/Phrases used primarily as synonyms for adult words
Adverts :	1 (1)	1 (1)	Advertisements
AllCaps :	0.3 (0.3)	0.5 (0.5)	Lots of capital letters
AOLURL :	1 (1)	1 (1)	Known or suspicious AOL URLs
ArentYouLucky :	1 (1)	1.5 (1.5)	Keywords for lottery win
AsciiArt :	1 (1)	1 (1)	Looks like ASCII art
attachdnsl :	1 (1)	1 (1)	Attachment MD5 in bin.vpop3.cc
AttachmentSpam :	1 (1)	1 (1)	Spam in an attachment

VPOP3 Enterprise 6.20 - Iml.pccs.co.uk - 192.168.66.23

The VPOP3 spam filter performs many checks on incoming messages. For simplicity, these tests are grouped into related 'rules' (eg, 'adultmisspelling' may test for 'sxe' and 'pr0n'). These different rules each

assign a 'score' to the message. These individual rule scores are added up to make a final score which VPOP3 uses to decide whether the message is spam or not.

When adding the rule scores together, VPOP3 first multiplies them by a 'weight' which lets the VPOP3 administrator adjust how important or not individual rules are. For instance, if you deal in pharmaceuticals the 'possibledrugs' rule may need to have its weight reduced, as you are likely to receive legitimate messages about viagra, etc (the 'drugmisspellings' rule is probably still wanted though, since 'v1@gra' is unlikely to be in a legitimate message even if you are a pharmaceutical company).

So, if the 'AllCaps' rule gives a message a score of '100' and the AllCaps rule weight is 0.3, then that rule will contribute a score of 30 (100 x 0.3) to the message's final spam score.

In general, a final spam score of 100 will cause a message to be marked as spam (but this can be changed if necessary).

The **Rule Weights** page lets you customise the weights for each of the rules defined by the spam filter. You can see each of the rules, the current and default weight values and a brief description of the rule. The values in parentheses are the default weights.

You can alter the rule weights by typing values into the boxes and pressing **Submit**. To reset the weights back to the default values you can either set them to the values in parentheses manually, or press the **Reset Default Weights** button to reset all the weights to default.

There are two columns of weights because the spam filter can use different values depending on other decisions. By default, VPOP3 will use the first column if the [Bayesian filter](#) decides the message is <=90% chance of being spam, and the second column if it decides the message is >90% chance of being spam.

(It is possible you may have more than 2 columns of weights. This can happen due to problems in the past. To fix this, you can edit the 'spamconfig.txt' file in the VPOP3 directory, to remove all the lines except those beginning with 'Config' and restart VPOP3. This will reset the rule weights to the defaults).

The individual rules are not described here because they can change over time. The Description column in the table gives a brief summary of what the rule is for. We cannot list the exact tests that a rule applies since they change over time and there may be thousands of tests for a single rule.

5.6.20.1.6 Advanced

To get to this page, go to Settings → Spam Filter → General → Advanced.

The screenshot shows the VPOP3 Admin Console interface. The left sidebar contains a tree view of settings categories, with 'Spam Filter' expanded to 'Advanced'. The top navigation bar includes links for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. The main content area is titled 'Spam/Content Filter' and has a 'Submit' button. Below the title bar are tabs for 'General', 'Quarantine Settings', 'Bayesian Database', 'Script Configuration', 'Rule Weights', and 'Advanced'. The 'Advanced Settings' section contains three checkboxes:

- Spam Filter uses Windows DNS resolution instead of VPOP3 method
- Use dynamic Spam Filter thread priority boosting
- Temporarily reject incoming SMTP on Spam filter timeout

 Below this is the 'Script Load Information' section, which includes a 'Reload files from disk' button and a table of loaded scripts.

File Path	Status
C:\vpop3\spamrules.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_initialise.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_user1.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_userlocal.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_localmail.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_userchecks.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_checks.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamddata_0.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamddata_1.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_dodns.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_dodns.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_userprocess.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_processresults.txt	Loaded OK (04/11/2016 11:50)
C:\vpop3\spamrules_userfinal.txt	Loaded OK (04/11/2016 11:50)

The Spam filter Advanced settings let you change settings you would normally never need to alter.

If the **Spam Filter uses Windows DNS resolution instead of VPOP3 method** option is checked, then VPOP3 uses the slower standard Windows method for resolving DNS 'A' records, rather than VPOP3's multithreaded high performance method. Usually this option should be turned off, but if the spam filter is having DNS problems it can be worth trying turning this option on instead. The VPOP3 spam filter performs a large number of DNS lookups on each incoming message. Occasionally because there is a large number of DNS queries performed very quickly this can upset a badly implemented DNS server, but this is rare nowadays.

The **Use dynamic Spam Filter thread priority boosting** option tells VPOP3 that if VPOP3 is processing several messages at once, once a message has been processed for several seconds, VPOP3 will boost the thread priority in Windows to try to get the message processed more quickly and avoid the spam filter from timing out. Usually this is checked.

The **Temporarily reject incoming SMTP on Spam filter timeout** option tells VPOP3 that if an incoming SMTP message causes the spam filter to timeout, then VPOP3 will send a temporary reject message to the sender to tell them to try again later. If this is not checked, then VPOP3 will accept the message without spam filtering it in this case. Usually if you have a large number of spam filter timeouts it means that you have configured VPOP3 to have too many incoming SMTP sessions for the server specifications. You should consider reducing the SMTP service's [Maximum incoming sessions](#) setting. Usually this option is checked.

The **Script Load Information** section displays if VPOP3 loaded the spam filter script files, and when it loaded them. Any errors are reported here. An error code of '2' indicates that the file is missing, which is probably OK, if the file is a 'spamrules_user.....' file because these are optional.

Note that the list of files can change on different installations. The only fixed file is the 'spamrules.txt' file, and that script file *includes* other files, so in different installations, different files may be *included*.

If you have had a problem such as a virus scanner blocking files or something, then pressing the **Reload files from disk** will trigger VPOP3 to reload the files, but that may not take place immediately. VPOP3 only checks to see if it should reload the files periodically to avoid a big performance hit.

5.6.20.2 White/Black Lists

The Spamfilter → White/Black Lists are where you can configure whitelist ("always allow") and blacklist ("always block") options for the VPOP3 spam filter

- [Whitelist Addresses Tab](#) - sender email addresses which should cause the message to be allowed
- [BlacklistAddresses Tab](#) - sender email addresses which should cause the message to be blocked
- [Whitelist Words Tab](#) - words/phrases which should cause the message to be allowed
- [Blacklist Words Tab](#) - words/phrases which should cause the message to be blocked

If a word or address is in both the Whitelist and Blacklist, then, by default they will cancel each other out. Precedence can be set by altering the list check [rule weights](#). For instance, if you want the whitelist to take precedence then you can set the **whitelist** rule weight to a bigger negative number than the **blacklist** rule weight is positive, such as setting the **whitelist** weight to -100 and the **blacklist** weight to 50. That means that if an address is in both lists, the blacklist will contribute 5000 to the final score and the whitelist will contribute -10000, meaning that the final score will be -5000, which will be passed through the filter as not spam.

The same can be done for the **WhitelistWords** and **BlacklistWords** rules.

5.6.20.2.1 Whitelist Addresses

To get to this page, go to Settings → Spam Filter → White/Black Lists → Whitelist Addresses

The screenshot shows the VPOP3 Enterprise 6.20 interface. The main window is titled "Spam/Content Filter" and displays the "Whitelist Addresses" section. The table below shows the following data:

Address	Added	Initially Added	Manually Added By	Last Added	Auto Added By	Add Count	Last Found	Find Count
	auto	2013-04-25 15:11:3		2013-04-25 15:11:3		1	2013-04-25 15:11:3	0
*@bounces.element5.com	manual	2016-03-10 12:24:0				0	2016-03-10 12:24:0	0
*@geocaching.com	manual	2007-08-01 14:06:5				0	2014-11-03 22:13:5	553
*@giffgaff.com	manual	2012-01-09 13:03:3				0	2016-07-13 21:21:4	648
	manual	2016-01-22 13:34:1				0	2016-07-11 07:55:2	7
	manual	2006-12-06 17:00:3				0	2016-03-09 04:14:3	70
	auto	2016-02-01 11:37:2		2016-02-05 07:52:2		4	2016-02-01 11:37:2	0
	auto	2014-05-28 07:15:3		2014-05-28 07:15:3		1	2014-05-28 07:15:3	0
	auto	2014-03-07 07:55:5		2016-07-06 06:53:5		2	2014-03-07 07:55:5	0
	auto	2012-07-15 19:16:5		2012-07-15 19:16:5		1	2014-08-02 22:57:4	5
	manual	2014-05-28 07:15:3		2016-03-16 11:14:3		2	2014-05-28 07:15:3	0
	manual	2013-06-29 07:34:3		2013-06-29 07:34:3		1	2013-06-29 07:34:3	0

Below the table, there is a form for "Entries to add:" and a "Bulk Delete Rules:" section with buttons for "Export", "Import", "Bulk Delete", and "Undo Last Bulk Delete (0 item(s))".

The Spamfilter Whitelist Addresses list contains sender email addresses which you want to be allowed through the spam filter. VPOP3 checks the From, Reply-To and Return-Path addresses.

By default, whenever a local user sends a message to an external email address, the recipient is added to the whitelist. This can be disabled by setting the [AutoWhiteList spamfilter setting](#) to '0'.

The table shows the entries already in the whitelist.

- The **Address** column shows the email address.
- The **Added** column shows whether the address was manually added by someone typing it in, or opting to add it when releasing a message from the [spamfilter quarantine](#), or automatically added when someone sent a message to that address.
- The **Initially Added** column shows when the address was initially added to the whitelist.
- The **Manually added by** column shows who manually added the address.
- The **Last Added** column shows when the address was last added (addresses may be automatically added multiple times, because they are added whenever someone sends a message to that address).
- The **Auto Added by** column shows the latest sender who caused the address to be automatically added.
- The **Add Count** column shows how many times the address has been automatically added.
- The **Last Found** column shows the latest time when the address was found as the sender of an incoming message.
- The **Find Count** column shows how many times the the address was found as the sender of an incoming message.

You can add new whitelist entries by typing them into the **Entries to add** box (one entry per line) and pressing the **Add new entries** button.

Note that when you add a new whitelist entry, VPOP3 will go through the [quarantine](#) and automatically release any already quarantined messages from that sender.

Also, note that, by default, VPOP3 will ignore whitelist entries for local senders. That is because these are not usually used as the senders for legitimate incoming email. You can change the **CheckLocalWhitelist** entry in the [spamfilter script configuration](#) to change this behaviour.

You can delete entries by selecting them and pressing the **Delete** button.

The **Show Filters** button will display boxes in the table headers where you can type search criteria. In the **Add Count/Find Count** filter boxes you can use numerical expressions, such as '<10' or '>100' etc.

Whitelist entries can be:

- complete email addresses which have to match totally
- [wildcard](#) email addresses (eg `*@example.com` or `*.sales@example.net`)
- [regular expressions](#) surrounded by `/` characters - eg `/^[a-m]*@example\.(com|net)$/`

The **Export** and **Import** buttons let you export or import the whitelist entries to a text file.

Bulk Delete Rules

The Bulk Delete Rules let you specify a rule to delete many whitelist entries at once.

The available rules are

1. auto - the entry was added automatically
2. manual - the entry was added manually
3. addcount <comparator> <number> - compare the addcount to the specified value. e.g. `addcount>100`
4. findcount <comparator> <number> - compare the findcount to the specified value. e.g. `findcount<75`
5. initiallyadded <comparator> <age> - compare the initially added date to the specified age. e.g. `initiallyadded<5years`
6. lastadded <comparator> <age> - compare the last added date to the specified age. e.g. `lastadded>6months`
7. lastfound <comparator> <age> - compare the last found date to the specified age. e.g. `lastfound>=2days`
8. addedby:<name> - compare the user which initially added the entry to the specified value (using wildcards). e.g. `addedby:fred*`
9. autoaddedby:<name> - compare the address which automatically added the entry to the specified value (using wildcards). e.g. `autoaddedby: *@yahoo.com`
10. matches:<regexp> - compare the entry address to the specified regular expression (case insensitive)
11. Any other value does a wildcard comparison of the value to the entry address

Do not put spaces around comparators, or after the colon character. Eg *addedby:fred** is valid, *addedby:fred** is not and will be treated as two separate conditions.

For ages, VPOP3 recognises the periods: *minutes, hours, days, months, years* (the 's' at the end is optional).

The comparators VPOP3 recognises are: *<, =, >, <=, >=, <>*

You should separate multiple conditions with space characters. All the specified conditions must match for the entry to be deleted. Once you have specified the conditions and pressed **Delete**, VPOP3 will tell you how many entries will be deleted, and will give you some examples of the entries which will be deleted. You can then confirm the deletion. If you find you have made a mistake, you can use the **Undo Last Bulk Delete** button to undo the latest bulk deletion (this only stores the deleted data for one day or until VPOP3 is restarted, whichever is the sooner).

5.6.20.2.2 Blacklist Addresses

To get to this page, go to Settings → Spam Filter → White/Black Lists → Blacklist Addresses

The screenshot shows the 'Spam/Content Filter' configuration page. The 'Blacklist Addresses' tab is active, displaying a table with the following data:

Address	Initially Added	Manually Added By	Last Added	Last Found	Find Count
/@_de/	2010-09-27 11:01:5			2010-09-27 11:05:5	3
bibble@bobble.com	2010-09-27 10:49:1			2010-09-27 11:04:4	2
sadsasd.com	2013-04-24 11:27:1	paul		2013-04-24 11:27:1	0

Below the table, there is an 'Entries to add' section with a text area and an 'Add new entries' button. At the bottom of the page, there are buttons for 'Export', 'Import', 'Bulk Delete Rules', 'Bulk Delete', and 'Undo Last Bulk Delete (0 item(s)) (help)'. The status bar at the bottom indicates 'VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23' and 'Idle | In: 44815 | Out: 0'.

The Spamfilter Blacklist Addresses list contains sender email addresses which you want to be blocked by the spam filter.

Generally, adding entries to the blacklist is not very useful because most spammers will fake the sender email address and generate random sender addresses.

The table shows the entries already in the blacklist.

- The **Address** column shows the email address.
- The **Initially Added** column shows when the address was initially added to the whitelist.
- The **Manually added by** column shows who manually added the address.

- The **Last Added** column shows when the address was last added since it was initially added.
- The **Last Found** column shows the latest time when the address was found as the sender of an incoming message.
- The **Find Count** column shows how many times the the address was found as the sender of an incoming message.

You can add new blacklist entries by typing them into the **Entries to add** box (one entry per line) and pressing the **Add new entries** button.

You can delete entries by selecting them and pressing the **Delete** button.

The **Show Filters** button will display boxes in the table headers where you can type search criteria. In the **Find Count** filter box you can use numerical expressions, such as '<10' or '>100' etc.

Blacklist entries can be:

- complete email addresses which have to match totally
- [wildcard](#) email addresses (eg `*@example.com` or `*.sales@example.net`)
- [regular expressions](#) surrounded by `/` characters - eg `/^[a-m]*@example\.(com|net)$/`

The **Export** and **Import** buttons let you export or import the blacklist entries to a text file.

Bulk Delete Rules

The Bulk Delete Rules let you specify a rule to delete many blacklist entries at once.

The available rules are

1. `findcount <comparator> <number>` - compare the findcount to the specified value. e.g. `findcount<75`
2. `initiallyadded <comparator> <age>` - compare the initially added date to the specified age. e.g. `initiallyadded<5years`
3. `lastfound <comparator> <age>` - compare the last found date to the specified age. e.g. `lastfound>=2days`
4. `addedby:<name>` - compare the user which initially added the entry to the specified value (using wildcards). e.g. `addedby:fred*`
5. `matches:<regex>` - compare the entry address to the specified regular expression (case insensitive)
6. Any other value does a wildcard comparison of the value to the entry address

Do not put spaces around comparators, or after the colon character. Eg `addedby:fred*` is valid, `addedby:fred*` is not and will be treated as two separate conditions.

For ages, VPOP3 recognises the periods: *minutes*, *hours*, *days*, *months*, *years* (the 's' at the end is optional).

The comparators VPOP3 recognises are: `<`, `=`, `>`, `<=`, `>=`, `<>`

You should separate multiple conditions with space characters. All the specified conditions must match for the entry to be deleted. Once you have specified the conditions and pressed **Delete**, VPOP3 will tell you how many entries will be deleted, and will give you some examples of the entries which will be deleted. You can then confirm the deletion. If you find you have made a mistake, you can use the **Undo**

Last Bulk Delete button to undo the latest bulk deletion (this only stores the deleted data for one day or until VPOP3 is restarted, whichever is the sooner).

5.6.20.2.3 Whitelist Words

To get to this page, go to Settings → Spam Filter → White/Black Lists → Whitelist Words

The screenshot shows the VPOP3 Enterprise 6.20 web interface. The left sidebar contains a tree view of settings, with 'Spam Filter' expanded and 'White/Black Lists' selected. The main content area is titled 'Spam/Content Filter' and has tabs for 'Whitelist Addresses', 'Blacklist Addresses', 'Whitelist Words', and 'Blacklist Words'. The 'Whitelist Words' tab is active, showing a table with one entry: 'Worldpay Order Information ('. Below the table is an 'Entries to add:' text box and an 'Add new entries' button. A note states: 'For performance reasons, at most 200 entries can be created in this list. Currently there is 1 entry.' Below this, instructions explain that entries can be plain text or regular expressions, and provide an example: '/bsexb/i' matches 'sex' but not 'Sussex'.

The Spamfilter Whitelist Words list contains words & phrases which you want to cause messages to be allowed through the spam filter. VPOP3 checks the message text & subject (not any attachments).

The table shows the entries already in the whitelist.

You can add new whitelist entries by typing them into the **Entries to add** box (one entry per line) and pressing the **Add new entries** button.

You can delete entries by selecting them and pressing the **Delete** button.

The **Show Filters** button will display boxes in the table headers where you can type search criteria.

Whitelist entries can be:

- simple words/phrases which have to match exactly as substrings of the message content
- [wildcard](#) text (eg `cat*basket`)
- [regular expressions](#) surrounded by / characters - eg `/bcat\b/`

Be aware that VPOP3 does not automatically match to word boundaries, so 'sex' will match 'sussex'. Use regular expressions with word anchors (`\b`) if you need to match at word boundaries.

Also, it is best if you are as specific as possible. If you just use simple words then they are likely to match where you do not expect.

5.6.20.2.4 Blacklist Words

To get to this page, go to Settings → Spam Filter → White/Black Lists → Blacklist Words

The screenshot shows the VPOP3 Enterprise 6.20 administration interface. The main content area is titled 'Spam/Content Filter' and has a green header bar. Below the header, there are four tabs: 'Whitelist Addresses', 'Blacklist Addresses', 'Whitelist Words', and 'Blacklist Words'. The 'Blacklist Words' tab is active. The main area contains a table with one entry: 'Estamos a procura de funcionarios'. Below the table, there is an 'Entries to add' text box and an 'Add new entries' button. A note explains that entries can be plain text or regular expressions, with an example: '/bsexb/i' matches 'sex' but not 'Sussex'.

The Spamfilter Blacklist Words list contains words & phrases which you want to cause messages to be blocked by the spam filter. VPOP3 checks the message text & subject (not any attachments).

The table shows the entries already in the blacklist.

You can add new blacklist entries by typing them into the **Entries to add** box (one entry per line) and pressing the **Add new entries** button.

You can delete entries by selecting them and pressing the **Delete** button.

The **Show Filters** button will display boxes in the table headers where you can type search criteria.

Blacklist entries can be:

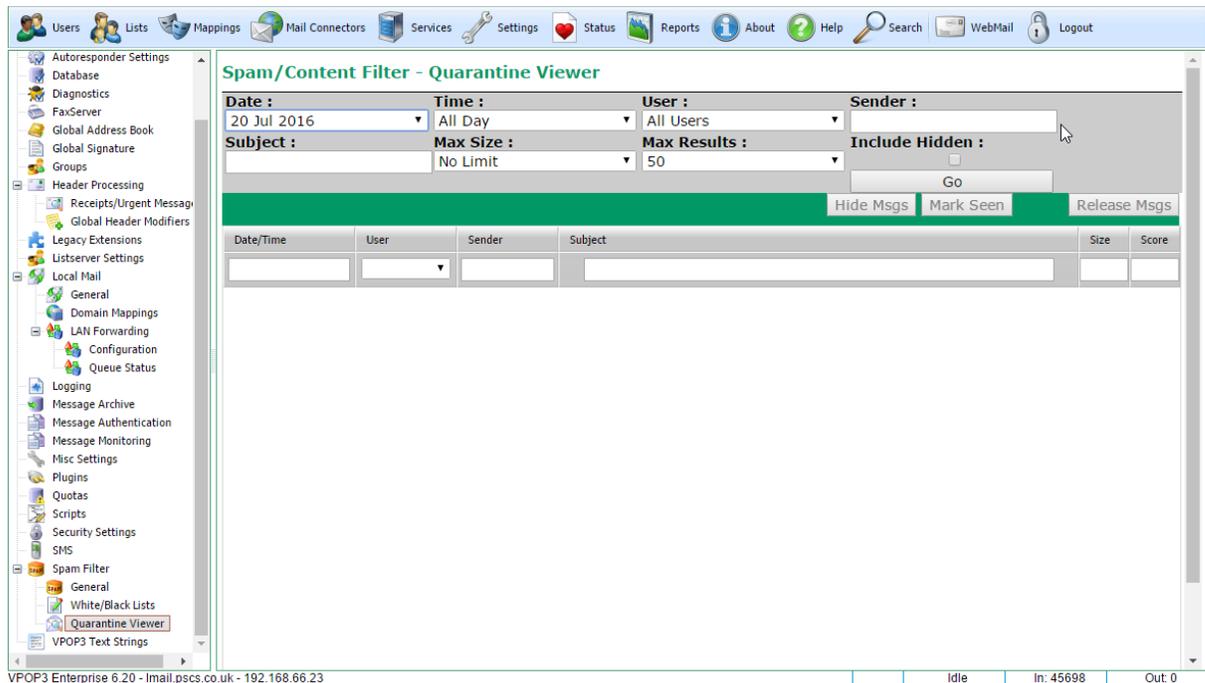
- simple words/phrases which have to match exactly as substrings of the message content
- [wildcard](#) text (eg `cat*basket`)
- [regular expressions](#) surrounded by / characters - eg `/bcat\b/`

Be aware that VPOP3 does not automatically match to word boundaries, so 'sex' will match 'sussex'. Use regular expressions with word anchors (`\b`) if you need to match at word boundaries.

Also, it is best if you are as specific as possible. If you just use simple words then they are likely to match where you do not expect.

5.6.20.3 Quarantine Viewer

To get to this page, go to Settings → Spam Filter → Quarantine Viewer



This page lets you view messages which have been caught by the VPOP3 Spamfilter [quarantine](#). You can also release messages, mark them as 'seen' or hide them.

First you must select the criteria for finding quarantined messages:

- **Date** - this is the date that the message was quarantined. VPOP3 keeps quarantined messages for a certain amount of time as configured in the [Quarantine Settings](#). You can select a specific date, or **All Dates**.
- **Time** - this is the time that the message was quarantined. You can select a time in hour steps, or choose **All Day** to search the entire day.
- **User** - this is the user whose quarantine the message is in. If you have used forwarding or the [Redirect spam filter script option](#), then this will be the target user, not the original user. You can choose **All Users** to search across all users
- **Sender** - this is text to search for in the sender's email address. This is matched using a substring match (wildcards are *not* allowed). If this is left blank, then all senders will match.
- **Subject** - this is text to search for in the email subject. This is matched using a substring match (wildcards are *not* allowed). If this is left blank, then all message subjects will match.
- **Max Size** - this is the maximum size of the original message to search for (or **No Limit**).

- **Max Results** - this is the maximum number of results to display. VPOP3 will display up to the specified number of quarantined messages. It sorts by "spamminess", so the most likely to be false positives will be selected first, then the most likely to be certain spam are selected last.
- **Include Hidden** - if you have hidden any quarantined messages, then this option will search in those messages as well.
- **Go** - press this button to search the quarantine for the specified criteria.

Once the search has completed so there are messages listed, you can filter them further by using the boxes at the top of the table. The **Size** and **Score** boxes support basic arithmetic comparators, eg < **100**. Note that these will only filter the results returned by the search, they will not perform further searches!

You can view a quarantined message by double-clicking on it. This displays the raw message, including the headers which is useful diagnostic information, including why the message was quarantined (see the *X-VPOP3-SPAM* header line).

You can 'Release' multiple messages at once by selecting them and pressing the **Release Msgs** button. Releasing messages will remove them from the quarantine and deliver them into the Inboxes of the user whose quarantine the messages are in.

The **Mark Seen** and **Hide Msgs** buttons are purely for personal housekeeping. Some people like to periodically go through the list and mark messages as read when they've checked them, other people just use the [daily quarantine reports](#) which are emailed out and only use this search facility if they are looking for a particular message. Marking messages as seen or hiding them has no effect on how VPOP3 works, the messages are still deleted when they have reached the appropriate age, whether or not they are hidden.

Releasing messages

When you select an individual message, the viewer displays it as below

Spam/Content Filter - Quarantine Viewer

Return-Path: <cpowell@pscs.co.uk>
 Authentication-Results: lmail.pscs.co.uk; spf=none; auth=none
 Received: from mail3.pscs.co.uk ([192.168.66.29]) by lmail.pscs.co.uk ([192.168.66.70] running VPOP3) with ESMTPS for <[redacted]>; Wed, 20 Jul 2016 01:05:54 +0100
 Authentication-Results: mail3.pscs.co.uk; spf=none; auth=none
 Received: from mail3.pscs.co.uk ([127.0.0.1] (localhost)) by mail3.pscs.co.uk ([127.0.0.1] running VPOP3) with ESMTMP for <[redacted]>; Wed, 20 Jul 2016 01:08:11 +0100
 DomainKey-Status: non-participant from=cpowell@pscs.co.uk; domainkeys=fail
 Received-SPF: Fail client-ip=187.235.186.158;
 envelope-from=cpowell@pscs.co.uk;
 helo=dsl-187-235-186-158-dyn.prod-infinitum.com.mx; identity=mailfrom
 Received: from dsl-187-235-186-158-dyn.prod-infinitum.com.mx ([187.235.186.158]) by mail3.pscs.co.uk ([192.168.66.29] running VPOP3) with ESMTMP for <cpowell@pscs.co.uk>; Wed, 20 Jul 2016 01:08:09 +0100
 From: <cpowell@pscs.co.uk>
 To: <cpowell@pscs.co.uk>

The X-VPOP3-SPAM header line indicates why the message was treated as spam.

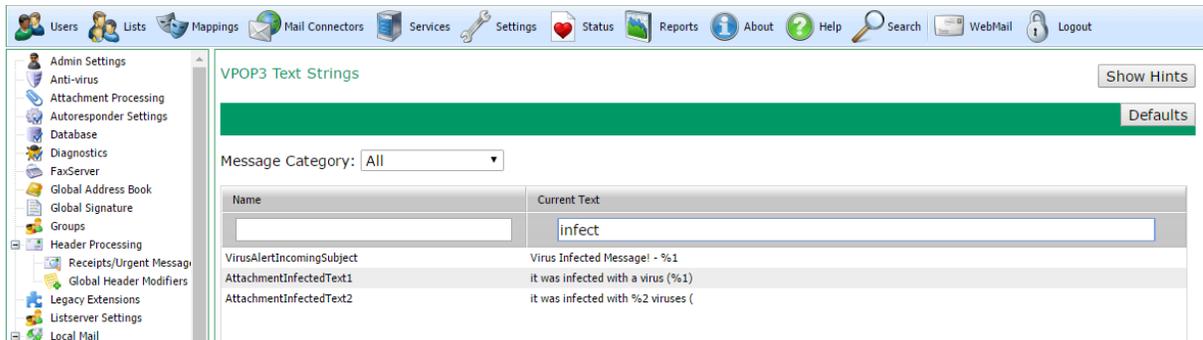
Train Bayesian filter as not spam Add sender (cpowell@pscs.co.uk) to to PSCS whitelist Report false positive to PSCS

If you decide to release the message, you can choose options with the three checkboxes at the bottom, then press the **Release Message** button.

- **Train Bayesian Filter as not spam** - this tells VPOP3 to train the [Bayesian Filter](#) that the message is not spam which will help improve its accuracy in the future.
- **Add sender <address> to whitelist** - this tells VPOP3 to add the message sender to the [Spamfilter Address Whitelist](#) for you, so that future messages from this sender will be allowed through.
- **Report false positive to PSCS** - this tells VPOP3 to forward a copy of the message to us so we can try to adjust the spamfilter so this sort of message will not be blocked in the future.

5.6.21 VPOP3 Text Strings

To get to this page, go to Settings → VPOP3 Text Strings

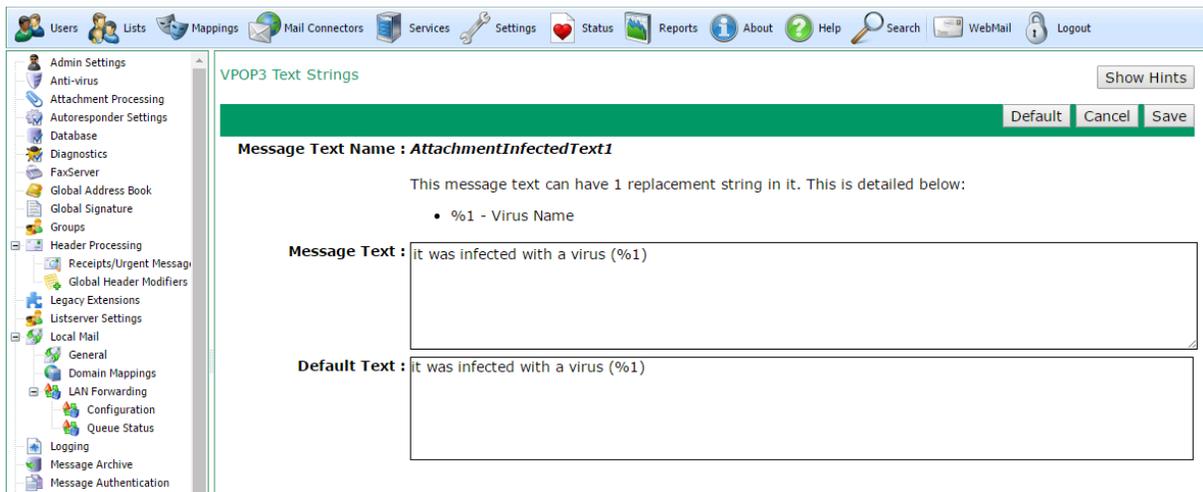


This page lets you customise the text used by VPOP3 in certain places. These are usually used in email messages generated or modified by VPOP3.

The **Message Category** drop-down lets you select a subset of the text strings, or **All** to show them all.

If you know the existing text, the easiest way to find the message you need to modify is to enter some of the known text in the filter box at the top of the **Current Text** column.

To edit text, double-click on the text you want to modify, you will be shown an editor, as below:



This will show the **Default Text** which is used on a normal VPOP3 installation. You can enter the text you want to use in the **Message Text** box, or press the **Default** button to set the Message Text to the Default Text.

Some text strings will have replacement text. In that case, the section above the Message Text box will display what replacements are available. If you wish you do not have to use all the available replacements, and you can use the same replacement multiple times.

Press the **Save** button to save the modified replacement. VPOP3 will use the new text immediately, VPOP3 doesn't need to be restarted.

5.7 Status

The status window displays live information about VPOP3's status.

There are three tabs:

- [Dashboard](#) - various bits of information displayed on one screen
- [Server Status](#) - VPOP3's connection status to the Internet for collecting & sending messages
- [Sessions](#) - Current connections to or from VPOP3

5.7.1 Dashboard

To get to this page, go to Status → Dashboard

The screenshot shows the VPOP3 Status Dashboard. At the top, there is a navigation bar with icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. Below this is a 'Status' window with a 'Submit' button. The dashboard is divided into three tabs: Dashboard, Server Status, and Sessions. The 'Dashboard' tab is active. It displays the following information:

- Connection Status:** Idle
- Last Connection:** 28 October 10:40:07
- Blocked IP addresses:** 2 (Latest added block: 1.1.1.3)
- Locked Users:** 0
- Database Connections:** 80 (represented by a horizontal bar chart)
- Active Sessions:** 50 (represented by a horizontal bar chart)
- Logged In Users:** 20 (represented by a horizontal bar chart)
- Last Update:** 27 October 12:00:03 - Result: 0
- Spamfilter:** Expires: 3 May 2036, Last check: 28 October 10:40:06, Last update: 28 October 10:40:06
- Outgoing Message Queue:** 0
- Next Connection:** 28 October 10:50:00
- System Messages:** A large empty box for displaying system messages.

At the bottom of the dashboard, there is a status bar showing: VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23 | Idle | In: 40188 | Out: 0

This tab shows a continuously updated summary of the VPOP3 status.

- **Connection Status** - current connection status - when VPOP3 is actively sending/collecting mail it is shown here. *Idle* does not indicate a problem, just that VPOP3 is not currently sending or collecting mail.
- **Outgoing Message Queue** - how many messages are waiting to be sent. Clicking on the number will take you to the [Outqueue viewer](#).
- **Last Connection** - the last time VPOP3 connected to send/collect mail.
- **Next Connection** - the next time VPOP3 will connect to send/collect mail. Clicking on the time will take you to the [Connection Schedule editor](#).
- **Blocked IP addresses** - the number of IP addresses which VPOP3 has blocked because of suspicious activity. The latest added IP address is also displayed. Clicking on this will take you to the

[Security Settings](#) where you can look at the Block List to see all the blocked IP addresses and remove them from there or add them to the never-block list.

- **Locked Users** - the number of user accounts which have been locked due to too many failed login attempts. Clicking on this will take you to the [Users list](#) where you can edit the user to unlock their account.
- **Database Connections** - the number of active database connections. This gives an idea of how loaded the VPOP3 server is. The green area is the maximum normal connections configured, and the red area is the number of extra connections VPOP3 can make in extreme circumstances. Normally the bar should be well within the green area. If it is constantly in or around the red area then it could indicate a disk performance problem on the VPOP3 server.
- **Active Sessions** - the number of active sessions to VPOP3 (e.g. user connections, incoming SMTP, collection & sending). The bar size will change as appropriate, so it being nearly full does not necessarily indicate that VPOP3 is overloaded.
- **Logged In Users** - the number of logged in user sessions to VPOP3. The bar size will change as appropriate, so it being nearly full does not necessarily indicate that VPOP3 is overloaded.
- **Last Update** - the last time VPOP3 checked for updates to itself and the result (0 = success).
- **Spamfilter** - details of the VPOP3 spam filter subscription, and update checks.
- **System Messages** - messages from VPOP3. You can mark messages never to be displayed again.

5.7.2 Server Status

To get to this page, go to Status → Server Status

The screenshot shows the VPOP3 Admin Settings interface. The navigation bar at the top includes icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. The main content area is titled "Status" and has a "Submit" button. Below the title are tabs for "Dashboard", "Server Status", and "Sessions". The "Server Status" tab is active, showing "Connection Status" as "Idle" with a "Connect Now" button. It also displays "Last Poll" and "Next Poll" times. A "Status Activity Log" shows a list of events, including duplicate detection and SMTP messages. At the bottom, there is a "Housekeeper Thread Status" section.

VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23

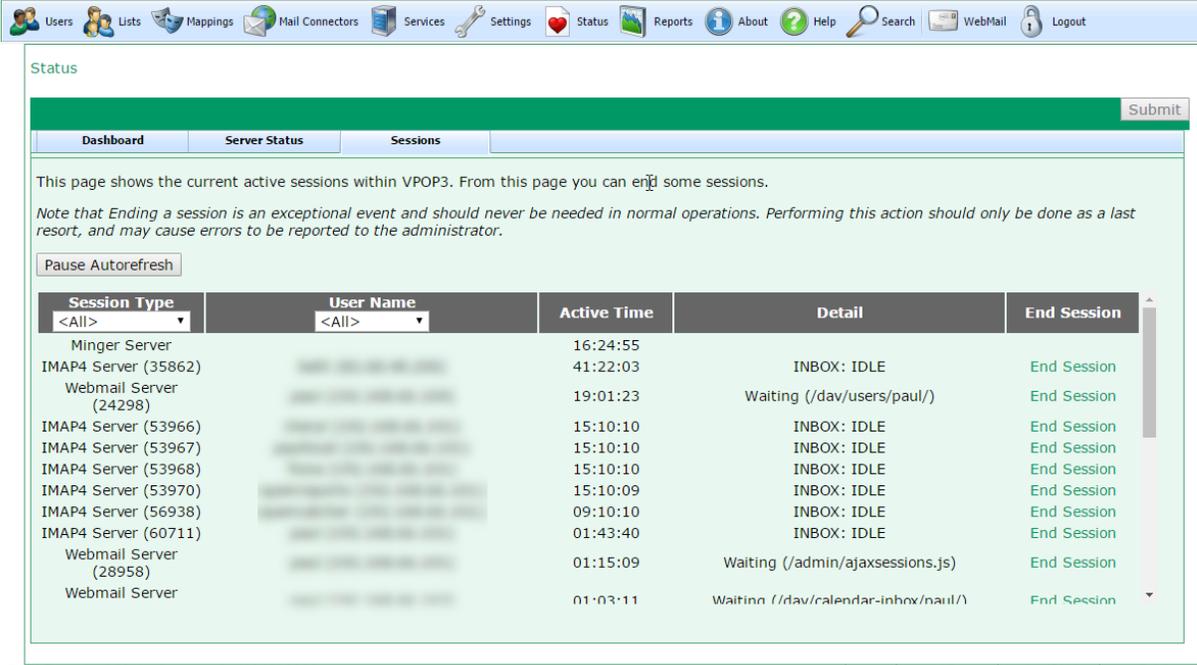
Idle | In: 45661 | Out: 2

This tab shows essentially the same information as the [VPOP3 Status Monitor](#).

- **Connection Status** - this shows the 'online' status of VPOP3. If it says idle, it does not mean VPOP3 is not working, or not doing anything, it just means that it is not currently sending or collecting mail from the Internet.
- **Connect Now** - Next to the Connection Status is a drop-down list of the Connections available, and you can press the Connect Now button to tell VPOP3 to connect to the selected Connection.
- **Last Poll** - this shows the time when VPOP3 last connected to the Internet to collect/send messages
- **Next Poll** - this shows the time when VPOP3 will next connect to the Internet to collect/send messages
- **Status Activity Log** - this shows a summary of recent activity by VPOP3, such as sending mail, retrieving mail, incoming SMTP messages, etc
- **Housekeeper Thread Status** - the Housekeeper Thread is a background task which performs actions such as sending daily reports. This section is for diagnostic/interest purposes, and can usually be ignored.

5.7.3 Sessions

To get to this page, go to Status → Sessions



The screenshot shows the VPOP3 Status page with the Sessions tab selected. The page title is "Status" and there is a "Submit" button in the top right. Below the navigation tabs (Dashboard, Server Status, Sessions), there is a "Pause Autorefresh" button. The main content area contains a table of active sessions. The table has the following columns: Session Type, User Name, Active Time, Detail, and End Session. The table lists several sessions, including Minger Server, IMAP4 Server (35862), Webmail Server (24298), and several IMAP4 Servers with IDs 53966, 53967, 53968, 53970, 56938, and 60711. The sessions are in various states: some are idle, some are waiting, and some are active. The footer of the page shows "VPOP3 Enterprise 6.20 - lmail.pscs.co.uk - 192.168.66.23" and "Idle | In: 45661 | Out: 2".

Session Type	User Name	Active Time	Detail	End Session
Minger Server		16:24:55		
IMAP4 Server (35862)		41:22:03	INBOX: IDLE	End Session
Webmail Server (24298)		19:01:23	Waiting (/dav/users/paul/)	End Session
IMAP4 Server (53966)		15:10:10	INBOX: IDLE	End Session
IMAP4 Server (53967)		15:10:10	INBOX: IDLE	End Session
IMAP4 Server (53968)		15:10:10	INBOX: IDLE	End Session
IMAP4 Server (53970)		15:10:09	INBOX: IDLE	End Session
IMAP4 Server (56938)		09:10:10	INBOX: IDLE	End Session
IMAP4 Server (60711)		01:43:40	INBOX: IDLE	End Session
Webmail Server (28958)		01:15:09	Waiting (/admin/ajaxsessions.js)	End Session
Webmail Server		01:03:11	Waiting (/dav/calendar-inbox/paul/)	End Session

This tab shows the current active sessions in VPOP3. This can be useful for seeing how busy VPOP3 is, or if someone is accessing VPOP3 from somewhere they shouldn't be, etc.

- **Session Type** - this shows the type of session, eg SMTP Server, IMAP4 Server etc. There may be a number in parentheses after the name, this is a session ID, and can be used to relate to diagnostic log file entries. The session IDs increment for each type of session separately, so can give an idea of how active VPOP3 has been.
- **User Name** - this shows the username, IP address, and/or any other identifying information which can be used to work out 'who' this session is for
- **Active Time** - this shows the time since the session was started (in hours:minutes:seconds)

- **Detail** - this shows information which may be useful to work out what the session is currently doing.
- **End Session** - Some sessions can be ended using the 'End Session' link. This terminates the TCP/IP connection associated with the session, and the session itself will terminate after it has noticed the resulting error, and has cleaned up, so it the session may not disappear from the list immediately.

You can filter the list by selecting entries in the **Session Type** and/or **User Name** table headers.

Usually the list periodically updates, but you can pause it by clicking the **Pause Autorefresh** button.

Possible Data

Session Type

- **Minger Server** - [Minger](#) is an address verification service. It is usually safe to leave this running, even if it is not in use, but you can administer it from the Services → SMTP Server → [Advanced](#) tab (Enterprise Only)

Detail

- **Waiting** means that the session is currently waiting for input from the client.
- **IDLE** in an IMAP4 session means that the session is currently in IDLE state, which is not the same as "Waiting". IDLE means the client has asked the server for notifications if anything changes in the currently selected folder.

5.8 Reports

The **Reports** section lets you run various reports on VPOP3 usage.

The available reports are:

- [Messages Received](#)
- [Messages Sent](#)
- [Message Summary](#)
- [Largest Folders](#)
- **Outgoing Message Counts**
- [Quotas](#)
- [SMTP Server Status](#)
- [SMTP Usage](#)
- [Spam Filter](#)
- **Users Last Login**

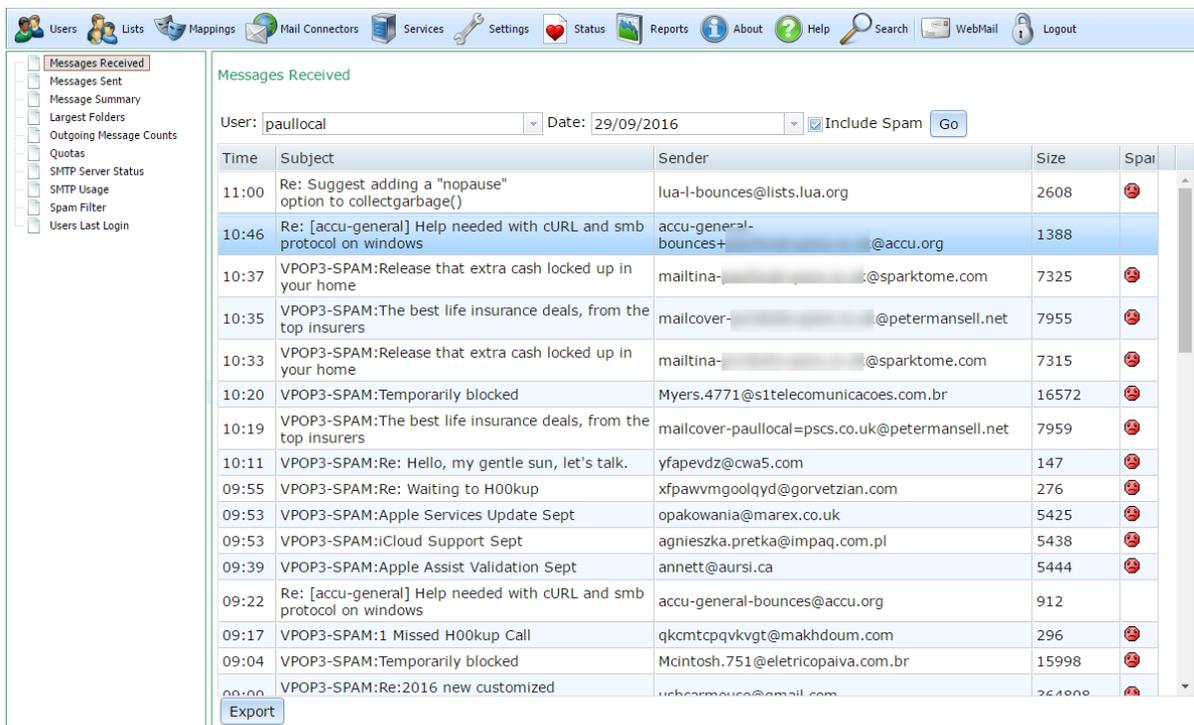
Some of these reports require [Historical Logging](#) to be enabled so that VPOP3 will track the required data.

Suggestion

We are always open to suggestions for other reports to add, as long as they will be generally useful to other VPOP3 users, not too complex, and the relevant data can be captured without adversely affecting performance or disk usage. Please contact us with your detailed suggestion. The current reports are reports which have been requested by users or which we have found useful ourselves.

5.8.1 Messages Received

To get to this page, to Reports → Messages Received.



The screenshot shows the VPOP3 web interface. The top navigation bar includes links for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. The left sidebar contains a tree view with 'Messages Received' selected. The main content area displays the 'Messages Received' report for user 'paullocal' on '29/09/2016'. The report includes a search bar with 'Include Spam' checked and a 'Go' button. Below is a table of messages:

Time	Subject	Sender	Size	Spam
11:00	Re: Suggest adding a "nopause" option to collectgarbage()	lua-l-bounces@lists.lua.org	2608	
10:46	Re: [accu-general] Help needed with cURL and smb protocol on windows	accu-general-bounces+@accu.org	1388	
10:37	VPOP3-SPAM:Release that extra cash locked up in your home	mailtina-@sparktome.com	7325	
10:35	VPOP3-SPAM:The best life insurance deals, from the top insurers	mailcover-@petermansell.net	7955	
10:33	VPOP3-SPAM:Release that extra cash locked up in your home	mailtina-@sparktome.com	7315	
10:20	VPOP3-SPAM:Temporarily blocked	Myers.4771@s1telecomunicacoes.com.br	16572	
10:19	VPOP3-SPAM:The best life insurance deals, from the top insurers	mailcover-paullocal=pscs.co.uk@petermansell.net	7959	
10:11	VPOP3-SPAM:Re: Hello, my gentle sun, let's talk.	yfapevdz@cwa5.com	147	
09:55	VPOP3-SPAM:Re: Waiting to H00kup	xfpawvmgoolqyd@gorvetzian.com	276	
09:53	VPOP3-SPAM:Apple Services Update Sept	opakowania@marex.co.uk	5425	
09:53	VPOP3-SPAM:iCloud Support Sept	agnieszka.pretka@impaq.com.pl	5438	
09:39	VPOP3-SPAM:Apple Assist Validation Sept	annett@aursi.ca	5444	
09:22	Re: [accu-general] Help needed with cURL and smb protocol on windows	accu-general-bounces@accu.org	912	
09:17	VPOP3-SPAM:1 Missed H00kup Call	qkcmtpqkvgt@makhdoum.com	296	
09:04	VPOP3-SPAM:Temporarily blocked	Mcintosh.751@eletricopaiva.com.br	15998	
09:00	VPOP3-SPAM:Re:2016 new customized	ueharmou@emil.com	26488	

At the bottom of the table is an 'Export' button. The status bar at the bottom shows 'VPOP3 Enterprise 6.20 - Imlai.pscs.co.uk - 192.168.66.23' and 'Idle | In: 39012 | Out: 0'.

This report lets you see which messages a specific user or email address received on a certain day. This report requires [Historical Logging](#) to be enabled.

Select the destination user in the **User** box, and the date in the **Date** box and press the **Go** button. If you check the **Include Spam** box, then the report will include quarantined messages as well.

The table will be completed with all the messages received through VPOP3 by that user. The time, subject, sender and message size are shown. If the message was quarantined, a red icon will be displayed in the **Spam** column

You can not view the message content itself because that is not logged due to space constraints. If you have Message Archiving enabled, you can search for the message in the [Message Archive](#).

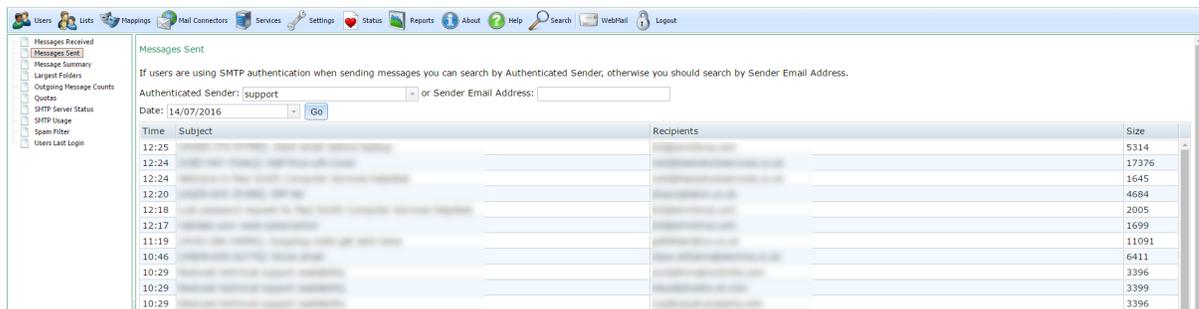
At the bottom of the page is an **Export** button which will let you download the table contents as a CSV file in case you want to load it into Excel or some other analysis software.

Suggestion

We are always open to suggestions for other reports to add, as long as they will be generally useful to other VPOP3 users, not too complex, and the relevant data can be captured without adversely affecting performance or disk usage. Please contact us with your detailed suggestion. The current reports are reports which have been requested by users or which we have found useful ourselves.

5.8.2 Messages Sent

To get to this page, to Reports → Messages Sent.



Time	Subject	Recipients	Size
12:25			5314
12:24			17376
12:24			1645
12:20			4684
12:18			2005
12:17			1699
11:19			11091
10:46			6411
10:29			3396
10:29			3399
10:29			3396

This report lets you see which messages a specific user or email address sent on a certain day. This report requires [Historical Logging](#) to be enabled.

If your users use SMTP authentication to send messages, then you can choose their username in the **Authenticated Sender** box, otherwise type the sender's email address into the **Sender Email Address** box. (If both boxes are populated, the **Sender Email Address** box is used). A common problem that people have is that they select a name in the **Authenticated Sender** box when they are not using SMTP authentication. In this case, the list may be empty or incomplete.

Then, select a date to look for in the **Date** box, and press the **Go** button.

The table will be completed with all the messages sent through VPOP3 by that user or email address. The time, subject, recipients and message size are shown. You can not view the message content itself because that is not logged due to space constraints. If the message was sent in the last day or two you can view recently sent messages in the [Outqueue Viewer](#) (this will also show if the message send succeeded, how many attempts were needed and so on), or if you have Message Archiving enabled, you can search for the message in the [Message Archive](#).

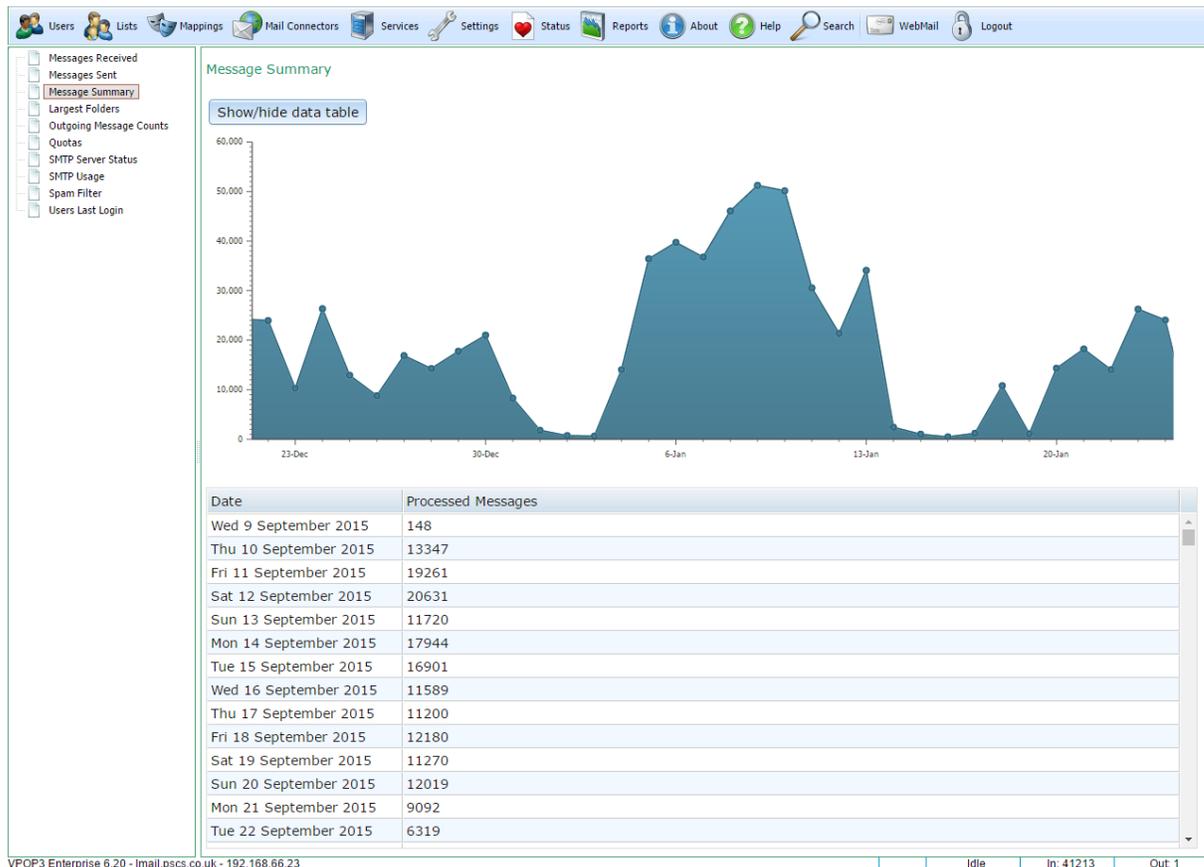
At the bottom of the page is an **Export** button which will let you download the table contents as a CSV file in case you want to load it into Excel or some other analysis software.

Suggestion

We are always open to suggestions for other reports to add, as long as they will be generally useful to other VPOP3 users, not too complex, and the relevant data can be captured without adversely affecting performance or disk usage. Please contact us with your detailed suggestion. The current reports are reports which have been requested by users or which we have found useful ourselves.

5.8.3 Message Summary

To get to this page, to Reports → Message Summary.



This report simply shows you a summary of counts of processed messages (incoming, outgoing and internal) against time.

This report requires [Historical Logging](#) to be enabled.

The graph is 'active'. If you hover the mouse over a data-point on the graph it will display the value at that time. You can use the scroll-wheel on your mouse to zoom in and out on the date axis, and, when zoomed-in, you can drag with the mouse to move the graph around.

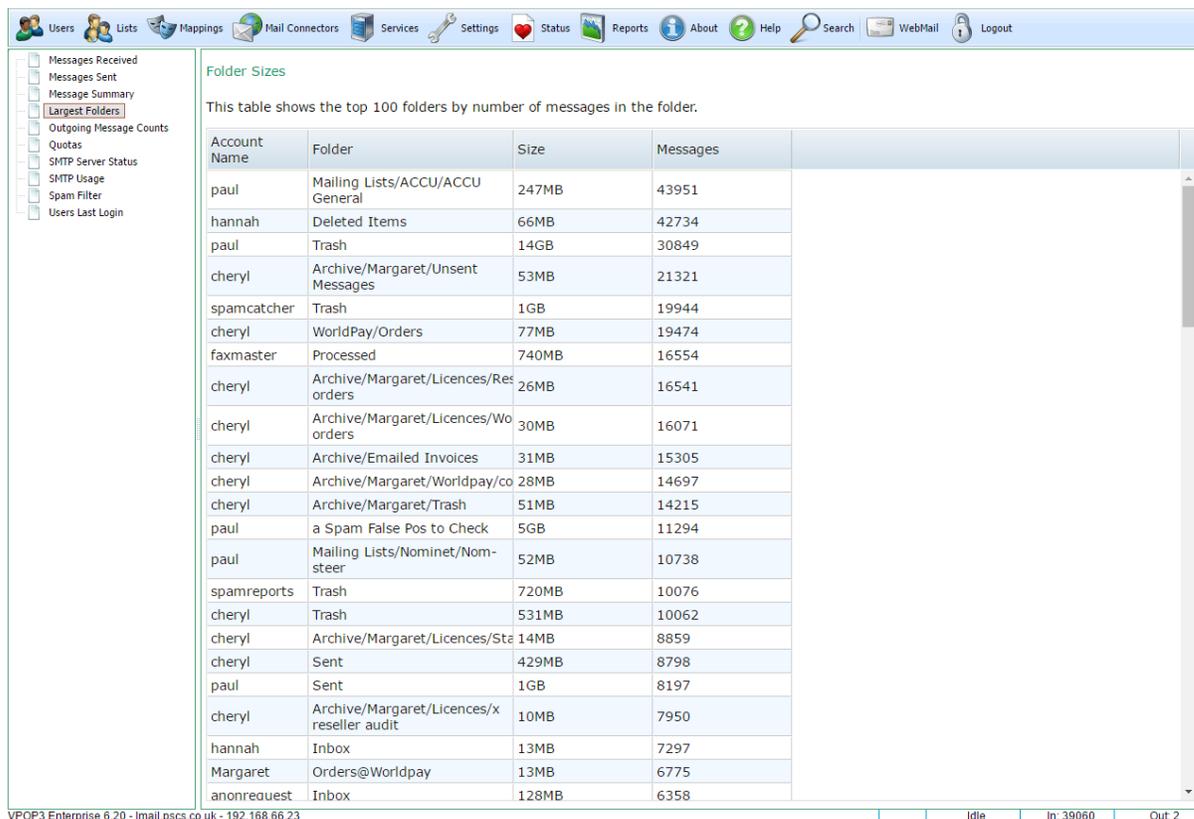
Below the graph is a table of data grouped by date. You can show or hide the table by clicking the **Show/hide data table** button.

Suggestion

We are always open to suggestions for other reports to add, as long as they will be generally useful to other VPOP3 users, not too complex, and the relevant data can be captured without adversely affecting performance or disk usage. Please contact us with your detailed suggestion. The current reports are reports which have been requested by users or which we have found useful ourselves.

5.8.4 Largest Folders

To get to this page, to to Reports → Largest Folders.



Account Name	Folder	Size	Messages
paul	Mailing Lists/ACCU/ACCU General	247MB	43951
hannah	Deleted Items	66MB	42734
paul	Trash	14GB	30849
cheryl	Archive/Margaret/Unsent Messages	53MB	21321
spamcatcher	Trash	1GB	19944
cheryl	WorldPay/Orders	77MB	19474
faxmaster	Processed	740MB	16554
cheryl	Archive/Margaret/Licences/Res orders	26MB	16541
cheryl	Archive/Margaret/Licences/Wo orders	30MB	16071
cheryl	Archive/Emailed Invoices	31MB	15305
cheryl	Archive/Margaret/Worldpay/co	28MB	14697
cheryl	Archive/Margaret/Trash	51MB	14215
paul	a Spam False Pos to Check	5GB	11294
paul	Mailing Lists/Nominet/Nom-steer	52MB	10738
spamreports	Trash	720MB	10076
cheryl	Trash	531MB	10062
cheryl	Archive/Margaret/Licences/Sta	14MB	8859
cheryl	Sent	429MB	8798
paul	Sent	1GB	8197
cheryl	Archive/Margaret/Licences/x reseller audit	10MB	7950
hannah	Inbox	13MB	7297
Margaret	Orders@Worldpay	13MB	6775
anonrequest	Inbox	128MB	6358

This report simply shows you a the 100 largest message folders counting the number of messages in the folder.

The table contains 4 columns:

1. The Account Name column shows the user name of the folder's owner.
2. The Folder column shows the folder name
3. The Size column shows the total folder size
4. The Messages column shows the number of messages in the folder

The table is initially sorted by number of messages, but you can sort the table by other columns by clicking on the appropriate column header.

Generally we recommend that common folders (eg Inbox, Sent Items etc) have fewer than 20,000 messages in them (preferably fewer than 10,000 - the fewer the better) because every time a user accesses that folder, their email client has to ask the server for a list of details of ALL the messages in that folder, so the more messages there are there, the more work is done by the server (and client) and the more data is transferred around.

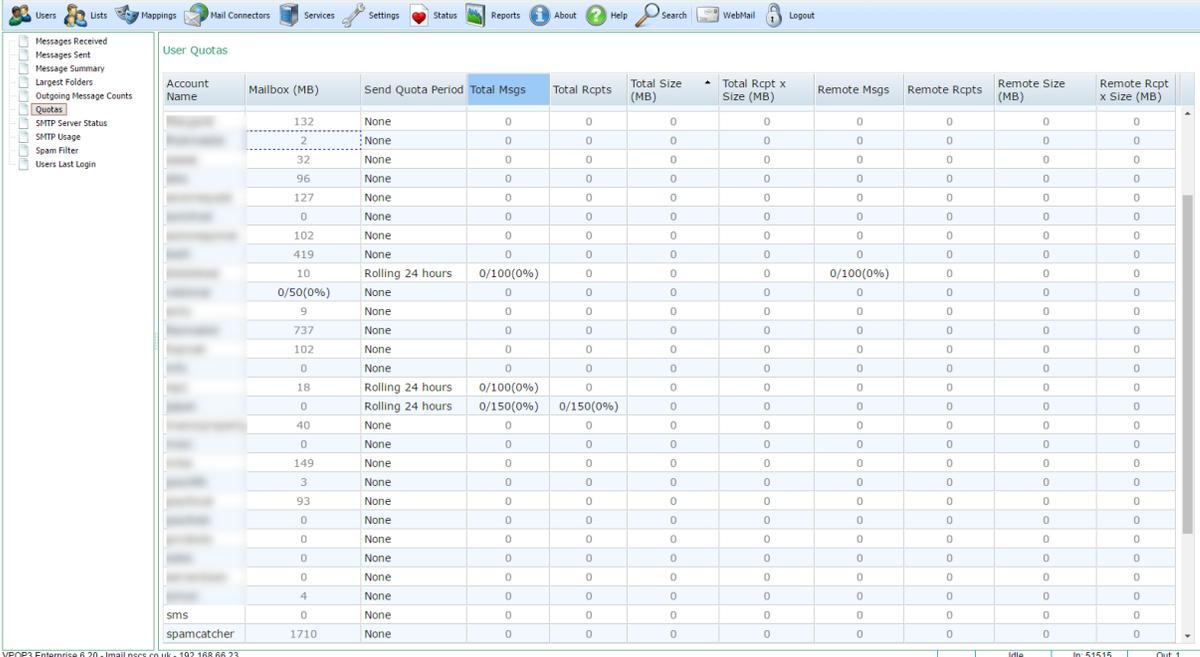
For folders which are accessed less often, then the folder size is not as important.

Suggestion

We are always open to suggestions for other reports to add, as long as they will be generally useful to other VPOP3 users, not too complex, and the relevant data can be captured without adversely affecting performance or disk usage. Please contact us with your detailed suggestion. The current reports are reports which have been requested by users or which we have found useful ourselves.

5.8.5 Quotas

To get to this page, to to Reports → Quotas



Account Name	Mailbox (MB)	Send Quota Period	Total Msgs	Total Rcpts	Total Size (MB)	Total Rcpt x Size (MB)	Remote Msgs	Remote Rcpts	Remote Size (MB)	Remote Rcpt x Size (MB)
	132	None	0	0	0	0	0	0	0	0
	2	None	0	0	0	0	0	0	0	0
	32	None	0	0	0	0	0	0	0	0
	96	None	0	0	0	0	0	0	0	0
	127	None	0	0	0	0	0	0	0	0
	0	None	0	0	0	0	0	0	0	0
	102	None	0	0	0	0	0	0	0	0
	419	None	0	0	0	0	0	0	0	0
	10	Rolling 24 hours	0/100(0%)	0	0	0	0/100(0%)	0	0	0
	0/50(0%)	None	0	0	0	0	0	0	0	0
	9	None	0	0	0	0	0	0	0	0
	737	None	0	0	0	0	0	0	0	0
	102	None	0	0	0	0	0	0	0	0
	0	None	0	0	0	0	0	0	0	0
	18	Rolling 24 hours	0/100(0%)	0	0	0	0	0	0	0
	0	Rolling 24 hours	0/150(0%)	0/150(0%)	0	0	0	0	0	0
	40	None	0	0	0	0	0	0	0	0
	0	None	0	0	0	0	0	0	0	0
	149	None	0	0	0	0	0	0	0	0
	3	None	0	0	0	0	0	0	0	0
	93	None	0	0	0	0	0	0	0	0
	0	None	0	0	0	0	0	0	0	0
	0	None	0	0	0	0	0	0	0	0
	0	None	0	0	0	0	0	0	0	0
	0	None	0	0	0	0	0	0	0	0
	4	None	0	0	0	0	0	0	0	0
sms	0	None	0	0	0	0	0	0	0	0
spamcatcher	1710	None	0	0	0	0	0	0	0	0

This report shows you the mailbox usage and quota usage of all your users. The table includes both mailbox size quotas and message sending quotas. These are configured in the **Quotas** tab of the user's settings.

The table can be sorted by clicking on a column header to sort by the values in that column.

The columns are:

- **Mailbox** - this shows the mailbox size.
- **Send Quota Period** - this indicates how the user's sending quota is defined (eg 24 hours, 1 month, etc) and whether it's a rolling or fixed period.

- **Total Msgs** - this indicates the total number of messages sent by that user within the **Send Quota Period** (or last 24 hours if no quota defined)
- **Total Rcpts** - this indicates the total number of recipients sent to by that user within the **Send Quota Period** (or last 24 hours if no quota defined)
- **Total Size** - this indicates the total size of messages sent by that user within the **Send Quota Period** (or last 24 hours if no quota defined)
- **Total Rcpts x Size** - this indicates the total of (message size multiplied by number of recipients) sent by that user within the **Send Quota Period** (or last 24 hours if no quota defined)
- **Remote Msgs** - this indicates the total number of outgoing messages sent by that user within the **Send Quota Period** (or last 24 hours if no quota defined)
- **Remote Rcpts** - this indicates the total number of outgoing recipients sent to by that user within the **Send Quota Period** (or last 24 hours if no quota defined)
- **Remote Size** - this indicates the total size of outgoing messages sent by that user within the **Send Quota Period** (or last 24 hours if no quota defined)
- **Remote Rcpts x Size** - this indicates the total of (outgoing message size multiplied by number of outgoing recipients) sent by that user within the **Send Quota Period** (or last 24 hours if no quota defined)

If there is a quota defined for any value for a user, the report also shows the quota size and the percentage used.

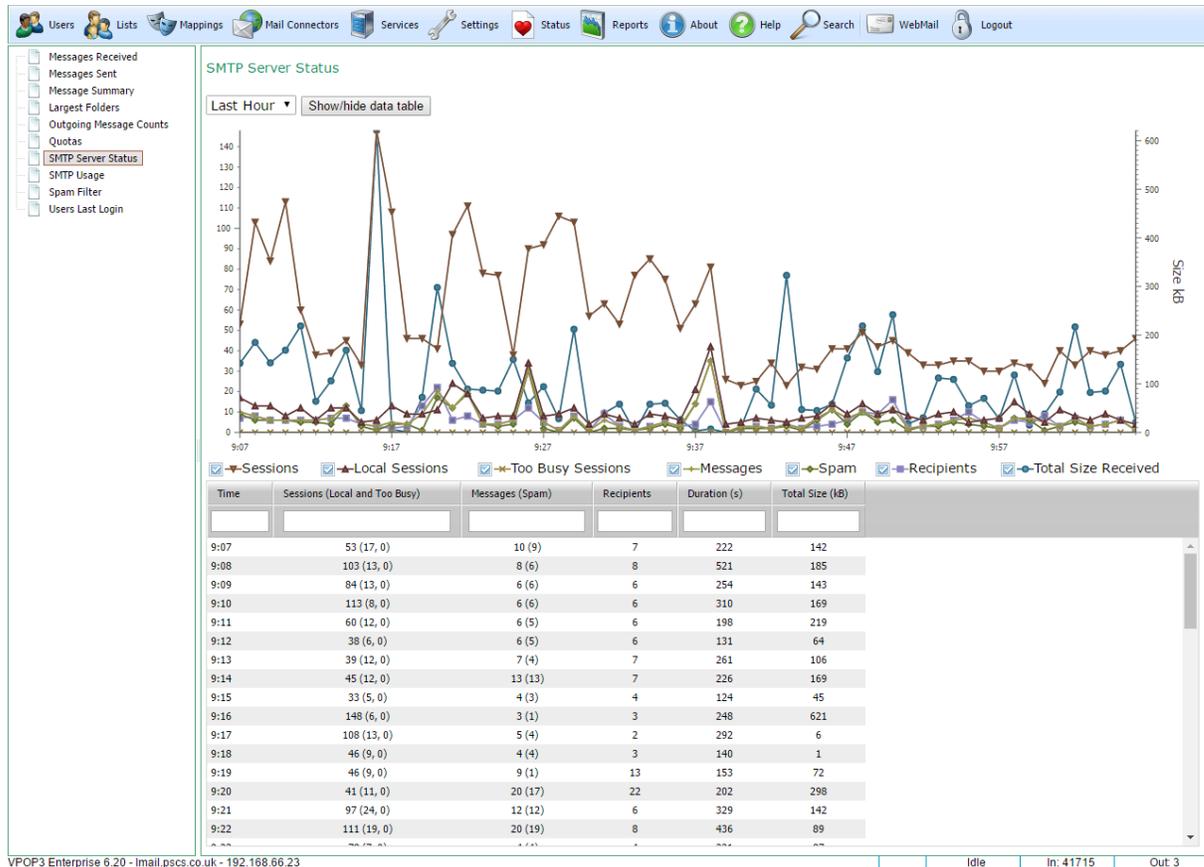


Suggestion

We are always open to suggestions for other reports to add, as long as they will be generally useful to other VPOP3 users, not too complex, and the relevant data can be captured without adversely affecting performance or disk usage. Please contact us with your detailed suggestion. The current reports are reports which have been requested by users or which we have found useful ourselves.

5.8.6 SMTP Server Status

To get to this page, to Reports → SMTP Server Status.



This report shows you a summary of recent activity to the VPOP3 SMTP service. This is for both incoming and local SMTP sessions.

The graph shows various data points:

- Sessions - this is the number of SMTP sessions which were started during the displayed time period.
- Local Sessions - this is the number of SMTP sessions which were made from local IP addresses.
- Too Busy Sessions - this is the number of SMTP sessions which VPOP3 ended because it was too busy (as configured on the SMTP Service [Load Limiting](#) tab).
- Messages - this is the number of messages sent through the SMTP service.
- Spam - this is the number of messages which VPOP3 detected as spam.
- Recipients - this is the number of recipients which VPOP3 was told to deliver messages to.
- Duration - this is the total time in seconds that the SMTP service was processing messages for.
- Total Size Received - this is the total size of messages.

This report does not require [Historical Logging](#) to be enabled, but can only display data for up to the last week.

The graph is 'active'. If you hover the mouse over a data-point on the graph it will display the value at that time. You can use the scroll-wheel on your mouse to zoom in and out on the date axis, and, when zoomed-in, you can drag with the mouse to move the graph around.

Below the graph is a table of data grouped by date. You can show or hide the table by clicking the **Show/hide data table** button.

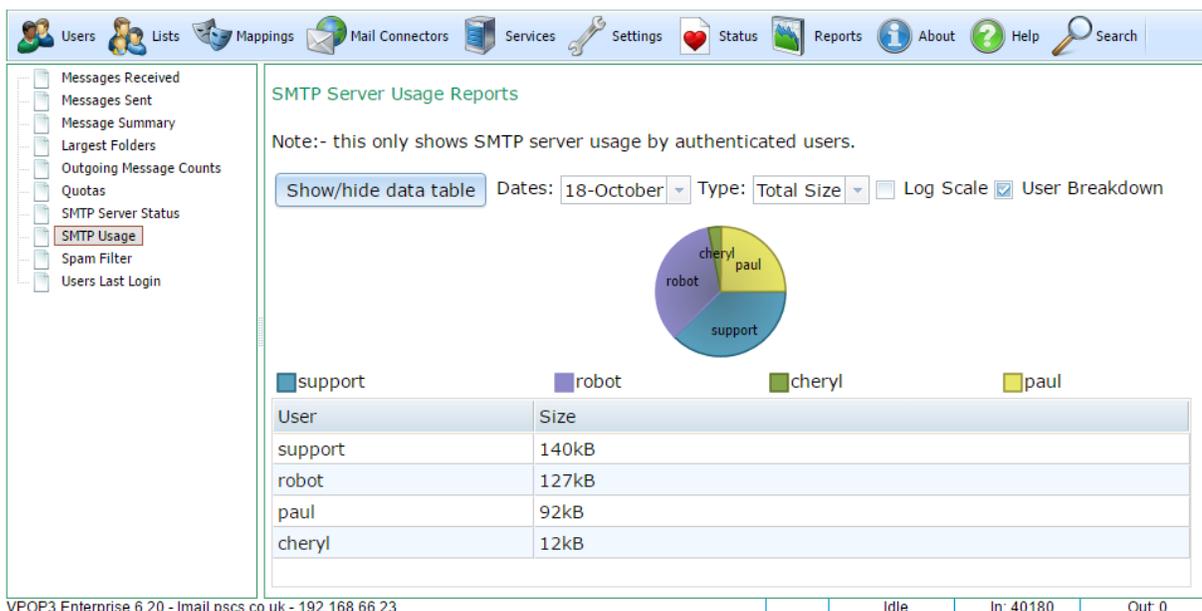
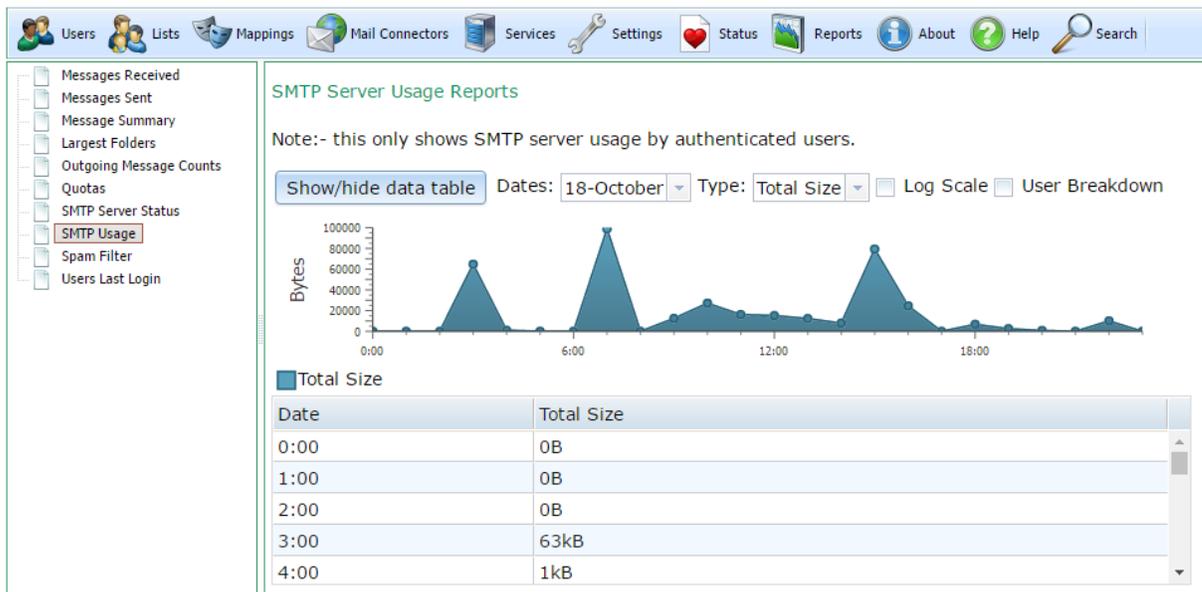


Suggestion

We are always open to suggestions for other reports to add, as long as they will be generally useful to other VPOP3 users, not too complex, and the relevant data can be captured without adversely affecting performance or disk usage. Please contact us with your detailed suggestion. The current reports are reports which have been requested by users or which we have found useful ourselves.

5.8.7 SMTP Usage

To get to this page, to Reports → SMTP Usage.



This report shows you a summary of recent SMTP service usage (i.e. sent messages) by authenticated users. It does not show incoming SMTP messages or unauthenticated users (use the Outgoing Message Counts or [SMTP Server Status](#) reports for that information, but it will be less detailed).

If **User Breakdown** is not checked, then this shows a graph of usage against time for the selected date(s). You can choose to show the number of messages sent, the size of messages sent, the number of recipients messages were sent to, or the total of recipients x size for the messages sent.

If **User Breakdown** is checked, then it shows a pie chart of the users' usage for the selected date(s). It does not show the graph against time. Only up to the top 20 users are shown.

If **Log Scale** is checked, then a logarithmic scale is used for the Y-axis, or for the pie-chart segment scaling. This reduces the effect of large differences in value making small values hard to detect. If **Log**

Scale is unchecked, then a linear scale is used. For instance, if the maximum size is 100,000 bytes, then a linear scale may show ticks at 0, 20000, 40000, 60000, 80000, 100000, where a logarithmic scale would show ticks at 1, 10, 100, 1000, 10000, 100000. A value of 100 would be hard to see on the linear scale, but easy on the logarithmic scale.

This report does not require [Historical Logging](#) to be enabled, but can only display data for the last month or two.

If you hover the mouse over a data-point on the graph it will display the value at that time

Below the graph is a table of data grouped by time/date/user. You can show or hide the table by clicking the **Show/hide data table** button.

Suggestion

We are always open to suggestions for other reports to add, as long as they will be generally useful to other VPOP3 users, not too complex, and the relevant data can be captured without adversely affecting performance or disk usage. Please contact us with your detailed suggestion. The current reports are reports which have been requested by users or which we have found useful ourselves.

5.8.8 Spam Filter

To get to this page, to Reports → Spam Filter.



This report lets you see a summary of counts of received messages against time and how many were detected as spam and how many were detected as not-spam by the VPOP3 spam filter.

This report requires [Historical Logging](#) to be enabled.

The graph shows the amount of not-spam messages in purple, spam messages in blue and the percentage of spam detected in green (as indicated by the legend below the graph).

The graph is 'active'. If you hover the mouse over a data-point on the graph it will display the value at that time. You can use the scroll-wheel on your mouse to zoom in and out on the date axis, and, when zoomed-in, you can drag with the mouse to move the graph around.

Below the graph is a table of data grouped by date. You can show or hide the table by clicking the **Show/hide data table** button.



Suggestion

We are always open to suggestions for other reports to add, as long as they will be generally useful to other VPOP3 users, not too complex, and the relevant data can be captured without adversely affecting performance or disk usage. Please contact us with your detailed suggestion. The current reports are reports which have been requested by users or which we have found useful ourselves.

5.9 About

To get to this page, go to About

The screenshot displays the 'About' page of VPOP3 Enterprise Version 6.20. The page includes a navigation bar at the top with icons for Users, Lists, Mappings, Mail Connectors, Services, Settings, Status, Reports, About, Help, Search, WebMail, and Logout. The main content area is divided into several sections:

- Section 1:** A box at the top stating 'This software is VPOP3 Enterprise Version 6.20 (build 2826)', 'Copyright ©1997-2014 Paul Smith Computer Services', and 'Built on Jun 27 2016 09:45:18'.
- Section 2:** A green box titled 'Licence Information' containing a table of details:

Licensed To:	PSCS
Maximum Users:	Unlimited
SMS Licence:	SMS PAYG Licence Entered
NNTP Service:	Not licenced
Spamfilter:	Licenced until 4 May 2036
VPOP3 Antivirus:	Licenced until 22 February 2018
Licence Activation:	Licence activation succeeded (Software maintenance expires on 2055-01-30)
- Section 3:** A button labeled 'Check/change Licence Details' located below the licence information table.
- Section 4:** A 'Support Information' box stating 'This software was supplied by' and 'For support:' with a bulleted list: 'Go to', 'Email', and 'Telephone'.
- Section 5:** A 'News' section with three items:
 - Reduced technical support availability** (13 July 2016): 'From 22nd July until 5th August (inclusive) there will be reduced technical support availability due to staff holidays. We ...'
 - VPOP3 v7 upcoming & beta-testers wanted** (4 June 2016): 'The next version of VPOP3 that we are planning will be version 7. We are changing from the 6.x sequence because we are planning ...'
 - New forum now open** (21 June 2016): 'We have just set up a new forum at <https://forum.pscs.co.uk> This is for suggestions, bug reports and general support for our ...'
 - VPOP3 v6.20 released** (8 June 2016): 'We have just released VPOP3 v6.20 which you can download from <http://www.pscs.co.uk/downloads/vpop3.php>. This is a free upgrade ...'

The footer of the page reads: 'VPOP3 Enterprise 6.20 - I-mail.pscs.co.uk - 192.168.66.23'.

This page shows information about your VPOP3 installation.

Section 1 shows the version number of VPOP3 and when it was built. (Note version numbers are not normal numbers, so 'version 6.20' is not the same as 'version 6.2').

Section 2 shows your licence information if any.

- **Licensed To** and **Maximum Users** shows your main VPOP3 licence details - who the software is licenced to and for how many users. This is all that is needed for VPOP3 to run.
- **SMS Licence** (optional) - this indicates whether you have purchased any pay-as-you-go Email -> SMS credits
- **NNTP Licence** (optional) - this indicates whether you have purchased an NNTP add-on licence
- **Spamfilter** (optional) - this indicates whether you have purchased a spam filter update subscription, and when it expires. The spam filter will continue to work after this date, but will not download updated definitions.
- **VPOP3 Antivirus** (optional) - this indicates whether you have purchased a VPOP3 Antivirus subscription, and when it expires. The virus scanner will stop working after this date.
- **Licence Activation** - this indicates whether VPOP3 has managed to verify your licence with our online activation servers, and, if so, when your Software Maintenance expires. See below for further information.

All the 'optional' licences above are optional, so if you do not have that licence, it does not mean there is a problem, just that you have not purchased that option.

Section 3 shows the button to view or change the VPOP3 licence details.

The screenshot shows a web form titled "Set VPOP3 Licence Details". At the top, there is a green bar with the title. Below this bar are two buttons: "Close" on the left and "Submit" on the right. The form contains several input fields: "Licence Owner : PSCS", "Licence Key : [blurred]", "Optional Keys" section with "SMS Licence : [blurred]" and "NNTP Key : [blank]", and a "Check For Upgraded Licence" button at the bottom.

The **Licence Owner** and **Licence Key** fields make up your VPOP3 licence details. You need to enter both of those exactly as provided by us. Letter case, punctuation, spaces etc are all important.

You can also enter the optional keys for the **SMS PAYG** service and **NNTP** service options here. If you have not purchased these options you can leave the boxes blank.

The **Check for Upgraded Licence** button lets VPOP3 search online for an upgraded licence for your installation.

Note that the **Spam Filter** and **VPOP3 Antivirus** subscriptions do not have licence keys. VPOP3 checks for updates using the main VPOP3 licence key which is validated online for the relevant subscription.

Any **Fax** licence is entered in Settings -> FaxServer

Section 4 shows support information. It should show who you purchased the software from, and support contact information for that provider. Note that the presence of contact information here does not mean you have free access to support. It may be that your provider needs you to pay for support.

Section 5 shows news about VPOP3. This is taken from a news feed from the [VPOP3 blog](#).

Licence Activation

Because we release a new version of VPOP3 every few months, we do not issue new licence keys for each version, otherwise it would get complex for us and users to manage. Instead, the same licence key is used, but has a 'maintenance expiry' date associated with it on our servers. When VPOP3 is installed or starts up it contacts these online servers to verify that the licence details it knows about are valid for this version of VPOP3. Once that is done, then the **Licence Activation** box will indicate **Licence Activation Succeeded**.

If VPOP3 cannot contact the activation servers, it will display **Licence Activation Pending** and VPOP3 will continue trying for some time before giving up. VPOP3 can be used as normal during this time.

For the activation to work, VPOP3 needs to be able to make outgoing HTTPS (TCP port 443) connections to the activation servers which are called **activate0.pscs.co.uk**, **activate1.pscs.co.uk** etc up to **activate7.pscs.co.uk**. If your VPOP3 installation does not have access to the Internet for some reason (this is rare, because email servers usually have Internet access to be most useful) then contact technical support for an alternative activation method which is less convenient but will work without Internet access.

6 Reference

This section contains reference material.

6.1 CIDR

CIDR stands for *Classless Inter-Domain Routing*.

In the past, IP addresses were allocated in 'classes' (eg 123.x.y.z was a Class A address, 197.31.x.y was a Class B address and 241.12.63.x was a Class C address). This meant that some organisations were getting far more IP addresses than they needed. For instance, even if you just needed 5 public IP addresses, you were allocated a Class C address, meaning you had 256 addresses, and if you needed 300, you were allocated a Class B meaning you had 65536 addresses, and if you needed more than 65536, you were allocated a Class A giving you over 16 million addresses.

In 1993, when it started to become clear that the Internet was going to be popular, it was realised that this was very inefficient and would lead to rapid exhaustion of IPv4 addresses. The IETF then introduced CIDR which is 'Classless' rather than the previous 'Classful' addressing. With CIDR, an address range can be any power of 2 size (1,2,4,8,16 etc). Because 2 IP addresses are reserved for the network address and broadcast address, and one is needed for a router, the '2' and '4' sizes are almost never used but they are still valid addresses. This meant it was far more efficient: if you need 5 addresses, you can be allocated an 8 address range, or if you need 300 you can be allocated a 512 address range. It is still wasteful, but this is necessary to allow fast performance from routers.

CIDR Notation

CIDR networks are often notated using as <network address>/<prefix size>. This is known as 'CIDR notation'.

The "prefix size" is the number of '1's in the subnet mask when written in binary.

So, for instance, a subnet mask of 255.255.255.0 can be written as 11111111 11111111 11111111 00000000 which has 24 '1's, so the prefix size is /24

So, a network address of 192.168.3.0 with a subnet mask of 255.255.255.0 would be written in CIDR notation as *192.168.3.0/24*

A single IP address of 192.168.3.72 could be written in CIDR notation as *192.168.3.72/32*

Common Subnet mask -> CIDR prefix size conversions

- 255.255.255.0 => /24
- 255.255.255.240 => /28
- 255.255.255.248 => /29

Technical information & IP routing

To understand CIDR and routing fully you need to understand basic binary mathematics and basic IP addressing.

Each IPv4 address consists of 4 numbers from 0 to 255. These can be written as 8 bit binary numbers
So, for instance, *192.168.72.15* can be written as 11000000 10101000 01001000 00001111

You may have encountered 'subnet masks'. In the above example, the subnet mask may be '255.255.255.0'.

255.255.255.0 can be written as 11111111 11111111 11111111 00000000

The CIDR "prefix size" is the number of '1's in the subnet mask when written in binary, so in the above case it would be 24.

CIDR uses the 'network address'. This is important because many problems are because people use host addresses in CIDR notation rather than the network address.

To determine the network address, you can perform a binary AND operation on the IP address and the subnet mask, this will give you the network address.

So, in the above example,

11000000 10101000 01001000 00001111 (*192.168.72.15*)

AND

11111111 11111111 11111111 00000000 (*255.255.255.0*)

results in

11000000 10101000 01001000 00000000 (*192.168.72.0*)

So, *192.168.72.0* is the network address for *192.168.72.15* with a subnet mask of *255.255.255.0*.

Note that *192.168.72.0* is NOT ALWAYS the network address if the IP address is *192.168.72.15*. The network address depends on the subnet mask as well. If the subnet mask was *255.255.255.248*, then you would do

11000000 10101000 01001000 00001111 (*192.168.72.15*)

AND

11111111 11111111 11111111 11111000 (*255.255.255.248*)

results in

11000000 10101000 01001000 00001000 (*192.168.72.8*)

So, in this case, the network address is *192.168.72.8*

The right-hand bits for a network address are always zeros.

The way network routing works, is that any IP aware device will do the binary AND operation to determine the network addresses for itself and the target device. If the network addresses are the same, then the two devices can communicate directly. If they are not the same, then the connection has to go via a router. These binary AND operations can be performed very quickly by computers so are efficient in high speed networking.

So, if 192.168.72.15 was trying to communicate with 192.168.72.182 and there is a subnet mask of 255.255.255.0 (CIDR prefix /24) on the source device, the source device will perform

```
11000000 10101000 01001000 00001111 (192.168.72.15)
```

AND

```
11111111 11111111 11111111 00000000 (255.255.255.0)
```

which results in

```
11000000 10101000 01001000 00000000 (192.168.72.0)
```

so, the source device knows that it's network address is 192.168.72.0, then it will perform

```
11000000 10101000 01001000 10110110 (192.168.72.182)
```

AND

```
11111111 11111111 11111111 00000000 (255.255.255.0)
```

which results in

```
11000000 10101000 01001000 00000000 (192.168.72.0)
```

The source device now knows that the target is on the same network as itself so it can communicate directly.

If 192.168.72.15 was trying to communicate with 15.25.83.11 and there is a subnet mask of 255.255.255.248 (CIDR prefix /29) on the source device, the source device will perform

```
11000000 10101000 01001000 00001111 (192.168.72.15)
```

AND

```
11111111 11111111 11111111 11111000 (255.255.255.248)
```

which results in

```
11000000 10101000 01001000 00001000 (192.168.72.8)
```

so, the source device knows that it's network address is 192.168.72.8, then it will perform

```
00001111 00011001 01010011 00001011(15.25.83.11)
```

AND

```
11111111 11111111 11111111 11111000 (255.255.255.248 - note it does not need to know the subnet mask for the target computer, it just uses its own subnet mask again here)
```

which results in

```
00001111 00011001 01010011 00001000 (15.25.83.8)
```

The source device now knows that the target is on a different network (15.25.83.8 or similar) from itself (192.168.72.8) so it knows it has to communicate via a router. It determines which router to use by consulting the Routing Table.

Routing Tables

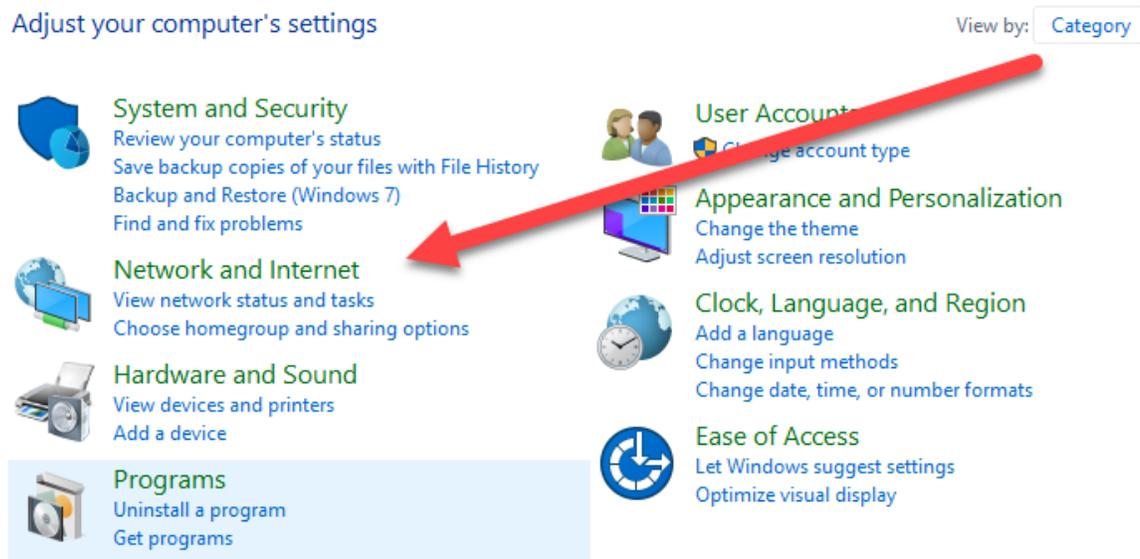
On each IP aware device there will be a 'routing table' which tells the device how to communicate with any other IP address. Many people are used to the 'default gateway', which is the fallback routing table entry if no other entry matches, but the routing table can contain many route entries. On Windows, the routing table can be viewed and manipulated using the *ROUTE* command at a command prompt, eg

ROUTE PRINT will display the routing table, or *ROUTE ADD* will add a routing table entry (use *ROUTE ?* to get basic help on the command).

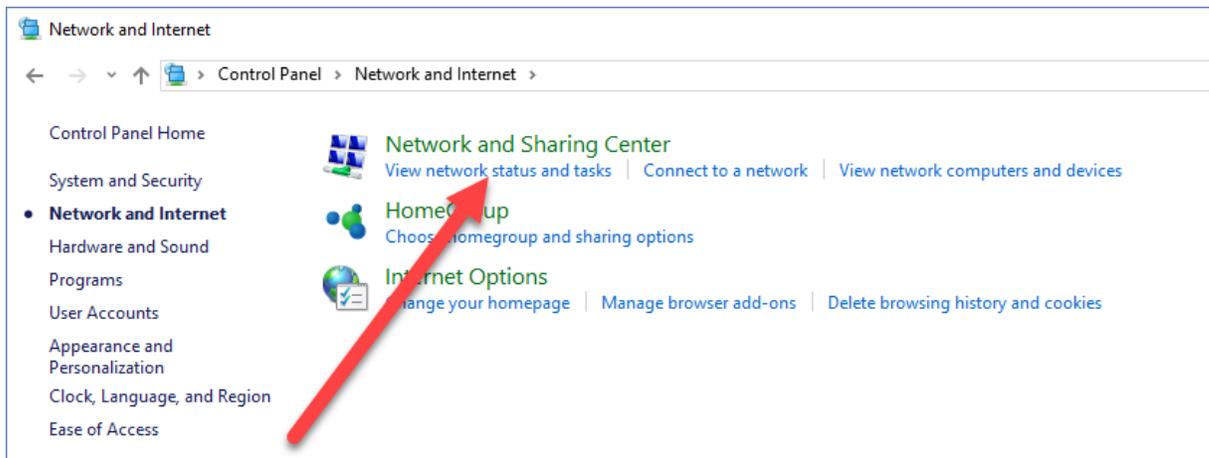
6.2 Creating a Dial-Up connection for VPOP3 to use

When creating a dial-up connection in Windows for VPOP3 to use, the important thing is that you *must* create the connection configured so that **anyone** can use it. If you don't say that anyone can use it, then it will just be associated with the 'current user'. Because VPOP3 runs as a service in a different user account, it will not be able to see any connections created for the current user. If you create the connection so that anyone can use it, then VPOP3 will be able to see and use it as well.

In Windows, open **Control Panel**



Select **Network and Internet**



Select **Network and Sharing Center**

View your basic network information and set up connections

View your active networks

pscs.co.uk
Domain network

Access type: Internet
Connections: Ethernet

Change your networking settings



[Set up a new connection or network](#)

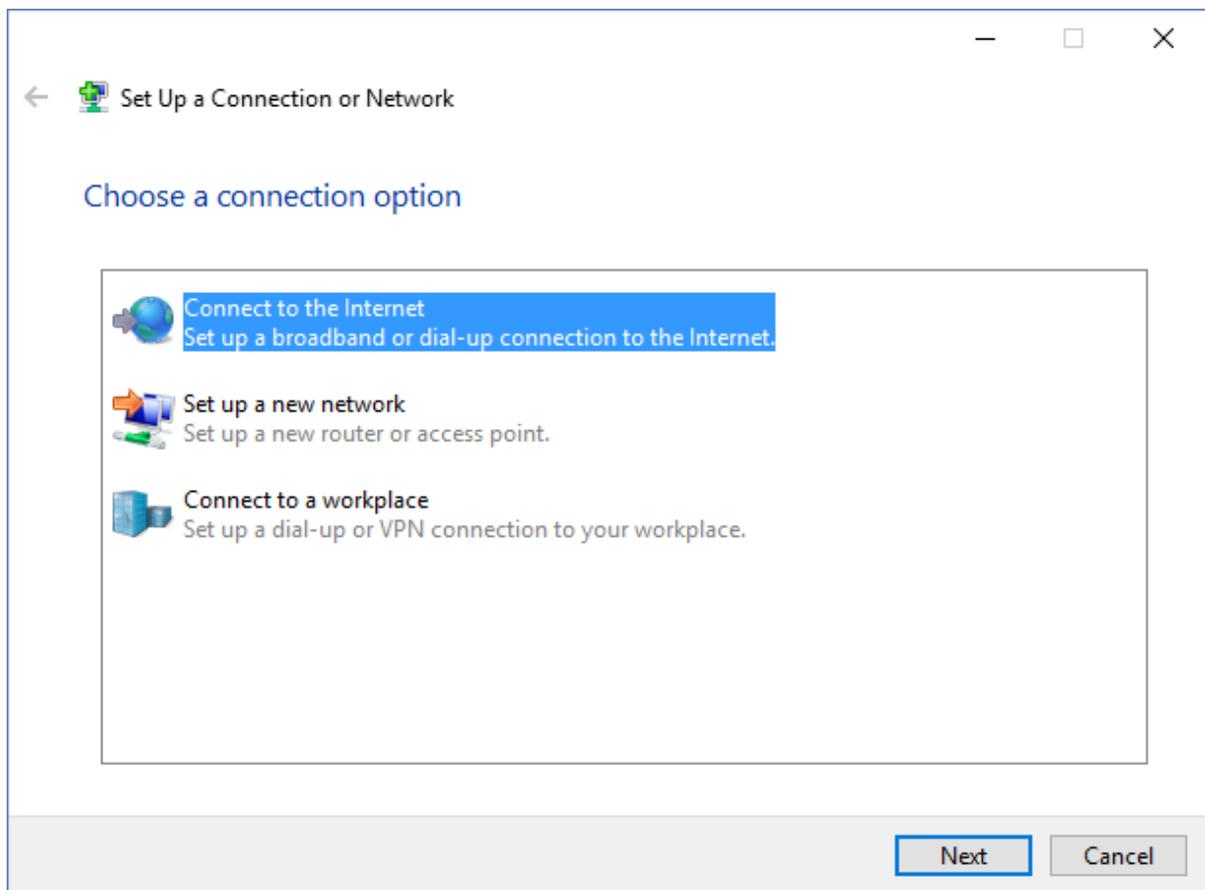
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.



[Troubleshoot problems](#)

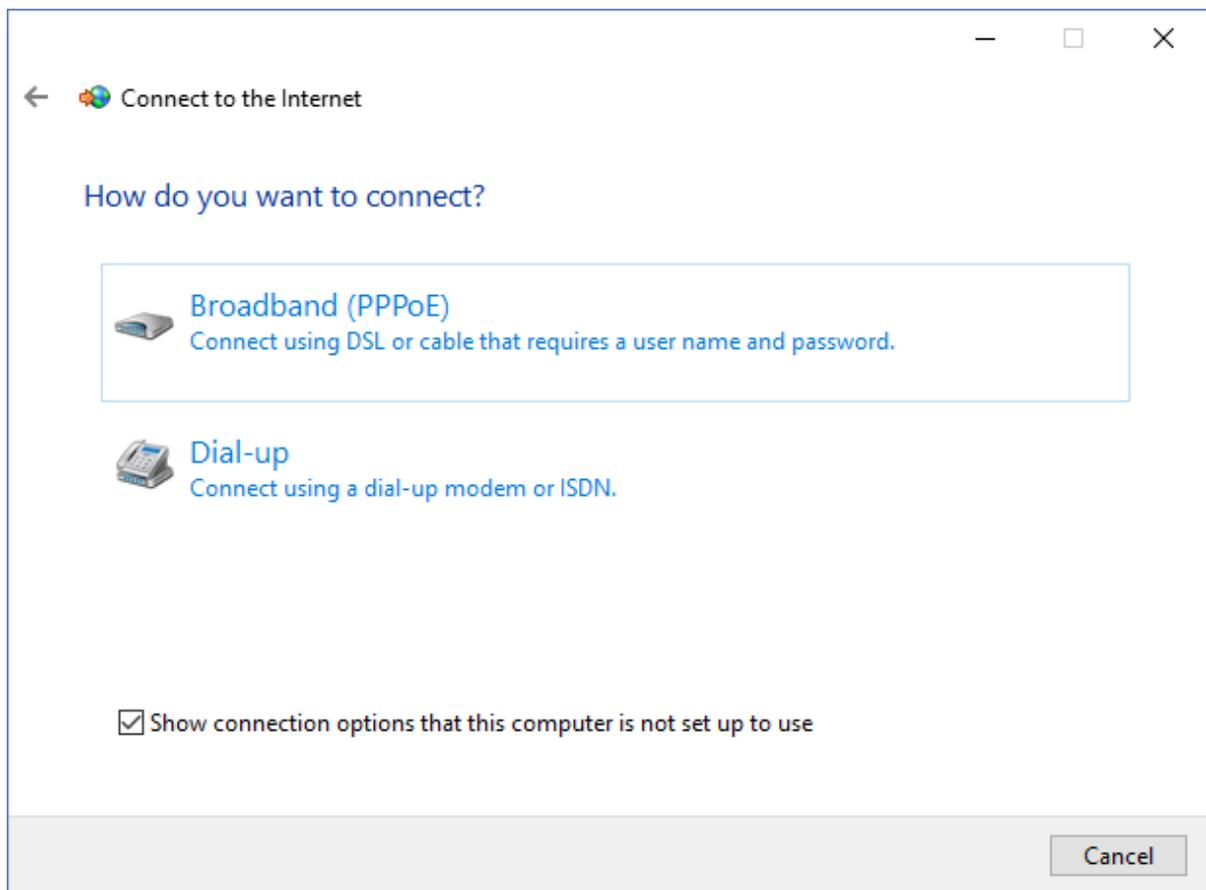
Diagnose and repair network problems, or get troubleshooting information.

Select **Set up a new connection or network**



Select **Connect to the Internet - Set up a broadband or dial-up connection to the Internet** and press **Next**.

If it says 'You are already connected to the Internet' choose **Set up a new connection anyway**.



Choose the appropriate method or modem

Connect to the Internet

Type the information from your Internet service provider (ISP)

Dial-up phone number: [Phone number your ISP gave you] [Dialing Rules](#)

User name: [Name your ISP gave you]

Password: [Password your ISP gave you]

Show characters

Remember this password

Connection name: [Dial-up Connection]

Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

[I don't have an ISP](#)

Create Cancel

Enter all the appropriate details provided by your Internet provider.

You **MUST** check the **Allow other people to use this connection** box.

Press **Create**.

Now, VPOP3 should be able to see this new dial-up connection.

6.3 Email File Types

Standard File Types

There are several common file types used with regards to email.

EML format

EML files are the most common type of email files. An EML file contains the raw message content. Most email software can export and import EML files simply, because that is how the messages are stored internally. For instance, in Mozilla Thunderbird, if you perform save as on a message, it will save it as an EML file.

Because the EML file format is the raw message content, all the Internet standards relating to message format such as [RFC 5322](#) apply to EML files as well.

MBOX format

MBOX files are 'mailbox' files. They are quite widely used in email software to store the contents of mail folders. An MBOX file is essentially a concatenation of all the email messages (in raw format).

[RFC 4155](#) describes the format of MBOX files.

MSG format

MSG files are the Microsoft proprietary format for saving files. Microsoft Outlook will save files as MSG files instead of the standard EML file format. Generally, of email clients, only Microsoft Outlook can read and write MSG files natively. There are utilities available for converting MSG files to EML files and vice versa. However, because Outlook converts messages into its own internal format for storage in its PST files, the MSG file often cannot be perfectly converted back into the original raw message, unless email clients which store messages in the original EML format (or in MBOX files)

6.4 File path macros

Where file or directory names can be defined in VPOP3 you can use some basic macros to help, especially if it is possible VPOP3 may be moved to another computer, because it will mean that the paths will automatically change.

The macros you can use are:

- %base% - this is the directory where VPOP3 is installed
- %htmlbase% - this is the directory where the Webmail/admin HTML files are stored (usually %base% _webmail)
- %appdata% - this is the Application Data folder for VPOP3 (eg c:\ProgramData\PSCS\VPOP3)
- %temp% - a temporary folder to use (eg c:\ProgramData\PSCS\VPOP3\Temp)

6.5 Lua Scripting

Lua is a scripting language. It is not as well known as Javascript etc, but it is much smaller and quicker and specifically designed for embedding in other software. It is widely used in applications ranging from industrial applications to games.

VPOP3 uses Lua in several places to allow user customisation to achieve features which are complex but not widely needed. Adding these features as core VPOP3 features would complicate it further for users who do not need these features and may still not achieve the flexibility that a full scripting language solution would offer.

Lua is documented fully on the Lua website at <http://www.lua.org>. VPOP3 currently uses Lua 5.2.

You can create & edit Lua scripts for VPOP3 in the Settings -> [Scripts](#) page. This includes an editor with Lua syntax highlighting. Alternatively, you can create .LUA files in the VPOP3 installation directory using any suitable text editor such as [Notepad++](#), [Sublime Text](#) or [UltraEdit](#).

When VPOP3 wants to use that script it will check in the VPOP3 installation directory for the relevant .LUA file. If it finds it, it will import the Lua file into the VPOP3 settings database and rename the .LUA file to .LUA.OLD. (It stores the scripts in the database so that backups & replication will backup & replicate the scripts automatically).

See the following topics for various places Lua scripts are used in VPOP3.

6.5.1 IDS Log Formatter Script

The IDS Log Formatter Script is a Lua script which can be used to generate a log file line for the [IDS \(Intrusion Detection System\) log file](#) generated by the SMTP service in reaction to certain events. This log file can be parsed by external software for reporting or automated firewall management.

Script Filename: *IDSLINE.LUA*

Function: *ProcessLine*

Syntax: *ProcessLine(<Client IP address>, <Event Type Number>, <Event Data>, <Format>, <Log File>)*

Returns: *<NewFormat>, <New Log File>*

If the function exists, then a 'do nothing' version of the function would be:

```
function ProcessLine(clientaddr, evttype, evtdata, format, logfile)
    return format, logfile
end
```

Parameters

- *Client IP Address* - IP address of the computer trying to send to VPOP3
- *Event Type Number* - defined in the [SMTP Server IDS topic](#).
- *Event Data* - context dependent data depending on the Event Type (eg the recipient address, bad command, etc)
- *Format* - the IDS log line format specified in the VPOP3 SMTP Server settings - will probably contain [text replacements](#)
- *Log File* - the IDS log file name specified in the VPOP3 SMTP Server settings

Return Values

- *Format* - the new log line format. This *may* contain [text replacements](#) but doesn't need to. If it does, then VPOP3 will process them as normal, but the ProcessLine function can return a fully formatted log line instead of a new format definition.
- *Log File* - the new IDS log file (may be the same as the parameter value, but the script may change it - eg for rotating log files etc).

6.5.2 Signature Script

The Signature Script is a Lua script which can be used to generate a signature (also known as a footer or disclaimer) for outgoing emails..

Script Filename: *SIGNATURE.LUA*

Function: *GetSignature*
Syntax: *GetSignature(<Format>, <Authenticated Sender>, <Sender Email Address>, <Subject>, <LDAP Attributes>)*
Returns: *<Signature text/HTML>*

This function is called whenever a local user sends an outgoing message.

Note that this function is *not* called if the sender authenticates when sending *and* the sender has the [signature option disabled](#).

Parameters

- *Format* - "HTML" or "PLAIN".
- *Authenticated Sender* - The VPOP3 username of the authenticated sender who sent the message (if any).
- *Sender Email Address* - The email address of the sender.
- *Subject* - The subject of the message.
- *LDAP Attributes* - If the sender used authentication, then this is a table containing the LDAP attributes for the sender.

Return Values

- *Signature Text* - the new signature to use. If this is blank, then VPOP3 will continue to generate a signature using the user's personal or the global signature from the VPOP3 settings. If you want not to have a signature, then the function should return the text "<blank>" (without the quotes, but with the angle brackets). If the *Format* is HTML, then the script should return an HTML segment, otherwise it should return a plain text segment.
-

Function: *GetInternalSignature*
Syntax: *GetInternalSignature(<Format>, <Authenticated Sender>, <Sender Email Address>, <Subject>, <LDAP Attributes>)*
Returns: *<Signature text/HTML>*

This function is called whenever a local user sends an internal message.

Note that this function is *not* called if the sender authenticates when sending *and* the sender has the [signature option disabled](#).

Parameters

- *Format* - "HTML" or "PLAIN".
 - *Authenticated Sender* - The VPOP3 username of the authenticated sender who sent the message (if any).
 - *Sender Email Address* - The email address of the sender.
 - *Subject* - The subject of the message.
-

- *LDAP Attributes* - If the sender used authentication, then this is a table containing the LDAP attributes for the sender.

Return Values

- *Signature Text* - the new signature to use. If this is blank, then VPOP3 will continue to generate a signature using the user's personal or the global signature from the VPOP3 settings. If you want not to have a signature, then the function should return the text "<blank>" (without the quotes, but with the angle brackets). If the *Format* is HTML, then the script should return an HTML segment, otherwise it should return a plain text segment.

6.5.3 SMTP Rule Scripts

The SMTP Rule Script is a Lua script which is called for every message received using SMTP to tell VPOP3 what to do with it. [SMTP Rules](#) are a simpler (but more restricted) way of doing this.

Script Filename: `SMTPRULES_x.LUA`

The 'x' in the filename is the SMTP service ID that this script is for. In VPOP3 Basic, this is always '1'.

In VPOP3 Enterprise for the default SMTP service it's '1'. It will be other numbers for any extra SMTP Services that have been created. To see the value of 'x' for extra SMTP services you have created, load `http://<server>:5108/admin/servicetree.js`. At the start of this page is a little list of all the services available. The first number on each row is the service ID.

The SMTPRULES_x.LUA scripts are different from other Lua scripts used by VPOP3 because most of the callback functions are not predefined. The [SMTP Rules](#) can call Lua functions themselves.

There are two predefined callback functions, and you can define others as you wish to be called from the SMTP Rules if certain conditions match.

VPOP3 calls the *Start* function at the start of the SMTP Rules process, and then the *Last* function at the end if no actions have been triggered for this message.

Each function has the same parameters/return values

Function: *First / Last / <custom>*
Syntax: *function(<Check Data>, <Size>, <TestPosition>, <Header Modifiers>, <Rule Name>)*
Returns: *<Action>, <Rule Number>, <Rule Name>, <Match Data>, <Header Modifiers>, <Block IP Address>, <Disconnect>, <Hold Message>, <Time Rule>*

Parameters

- *Check Data* - Table of:
 - *MailFrom* - return path (sender's email address)
 - *ClientIPAddress* - sender's IP address

- *AuthUser* - authenticated sender's username (if any)
- *HeaderFrom* - the email address from the 'From' message header
- *HeaderFromTextName* - the text name from the 'From' message header
- *Subject* - the message subject
- *Recipients* - table of message recipients
- *BccRecipients* - table of message BCC recipients (if any)
- *Header* - table of message header lines
- *Size* - The message size in bytes
- *TestPosition* - At what point the SMTP Rule test is happening: 1 = MAIL FROM, 2 = RCPT TO, 3 = DATA
- *Header Modifiers* - Any existing header modifiers to be applied to the message
- *Rule Name* - The SMTP Rule name being processed

Return Values

- *Action* - a numeric value of:
 - 0 - do nothing (default action, or let some other rule do something)
 - 1 - accept the message
 - 2 - reject the message
 - 3 - redirect the message to another address
 - 4 - ignore the message (accept it, but don't deliver it)
 - 5 - copy the message to another address
- *Rule Number* - for logging
- *Rule Name* - for logging
- *Extra Data* - for redirect/copy actions this is the address to redirect/copy the message to. If Block IP Address is set, this is the time in minutes that the IP address should be blocked for.
- *Header Modifiers* - Table of header modifiers (should be the passed in 'Header Modifiers' value if no changes wanted)
- *Block IP Address* - boolean - add the 'ClientIPAddress' to the [Blocked IP Address](#) list.
- *Disconnect* - boolean - if this is true, then the SMTP connection will be dropped after this message has been processed
- *Hold Message* - boolean - if this is true, then if the message is accepted, it will be 'held' afterwards, so a local recipient cannot access the message and outgoing messages will not be sent
- *Time Rule* - boolean - if this is true, then a reject will be given as a temporary reject code asking the sender to try again later (eg if you want to delay the message delivery for some reason)

6.6 PostgreSQL installation details

VPOP3 uses PostgreSQL as its back-end database. This database stores everything from settings to message content. The only things currently not stored in the database are quarantined messages and archived messages (future versions of VPOP3 may store quarantined messages in the database as well).

VPOP3 v5 and later require PostgreSQL 9.1 or later. VPOP3 v7 and later require PostgreSQL 9.5 or later.

The VPOP3 installer will install a copy of PostgreSQL in the 'pgsql' subdirectory of the VPOP3 installation folder. It is installed as a Windows service called **VPOP3DB** which runs as a Windows user called **vpop3postgres**. For security, this Windows user has full permissions to the 'VPOP3\pgsql\data' directory, read only access to the other 'VPOP3\pgsql' directories, and no access elsewhere on the disk

Custom installation of PostgreSQL

The installation of PostgreSQL into the VPOP3 directory is purely for ease of use and installation: it is *not* important for VPOP3 that it is installed this way. In fact, the PostgreSQL server could be installed in another directory or drive on the same PC, or even on a different PC. You could install PostgreSQL on a Linux computer or NAS server or whatever, as long as it is of an appropriate version and has suitable performance (including network connectivity).

This section of the manual is for advanced users who may want install PostgreSQL elsewhere. It will not go into step-by-step details - if you need those, then you should probably not be doing this, but it is there for advanced users who may know about PostgreSQL and want to install it in a different location or different PC and just need to know what VPOP3's requirements are.

As mentioned, VPOP3 requires PostgreSQL 9.1 or later for VPOP3 version 5 or 6.x and PostgreSQL 9.5 or later for VPOP3 version 7 or later. Note the 'or later's, so you *could* use PostgreSQL 9.3 with VPOP3 version 5, and it will work fine. VPOP3 requires features added in the mentioned versions of PostgreSQL, but those features are present in later versions of PostgreSQL as well.

The VPOP3 installer installs a 32 bit version of PostgreSQL, but you can use a 64 bit version without any problems at all.

The requirements for an installation of PostgreSQL to be used with VPOP3 are:

- It must be an appropriate version of PostgreSQL
- There must be a PostgreSQL user/role created which needs a password to log in. This must be the owner of the database VPOP3 uses.
- The database must be created with the 'SQL_ASCII' encoding (eg 'CREATE DATABASE vpop3 ENCODING 'SQL_ASCII' TEMPLATE template0;')
- The database must be accessible from the VPOP3 computer (ie set the 'pg_hba.conf' file correctly)

If you do this before installing VPOP3, then tell the VPOP3 installer that you don't want to install the Database component. It will then ask you for database connection information.

If you do this after installing VPOP3, then you should migrate the database over to the new database by using a pg_dump/pg_restore process. You can then [edit the VPOP3.INI file](#) to set the database connection settings.

6.6.1 vpop3postgres user account

When VPOP3 is installed, the installer creates a Windows user called **vpop3postgres**. The PostgreSQL database service (VPOP3DB) is run as this user.

The user is created as a local user on all installations of Windows except where VPOP3 is installed on an Active Directory controller. In that case, it is created as a domain user (Active Directory controllers do not have local users, so it must be created as a domain user).

You should not remove this Windows user unless you *really* know what you are doing, and doing so is unsupported.

The **vpop3postgres** user is removed from the Users/Domain Users group so should have no permissions other than those specifically created by the VPOP3 installed (i.e. access to the VPOP3\pgsql folder).

The default password for the **vpop3postgres** user is "Nc6ACboDt2jVL6". It is possible to change this as long as the login details for the VPOP3DB service are also changed. Note that changing it may cause issues during upgrades (because the installer has to perform certain tasks by running programs as that user (which requires the password)), or upgrades may reset it back to the default password (to prevent any problems).

6.7 Regular Expressions

Regular Expressions are a common way of expressing a "pattern" for matching/searching text. People may be familiar with * and ? 'wildcards'. Regular Expressions are much more powerful than that. There are many tutorials on the Internet for Regular Expressions. <http://www.regular-expressions.info/> is one we know.

A Regular Expressions is also known as a regex or regexp.

There are several 'flavours' of regular expressions. VPOP3 uses Perl Compatible Regular Expressions (PCRE) most of the time. (Lua scripting uses Lua's native pattern matching).

The simplest regular expression is just some text, so the regular expression **cat** will match the words *cat*, *catch*, *caterpillar*, *abdicate*, etc. Regular expressions are usually case sensitive, unless indicated otherwise.

Often regular expressions are entered with / characters around them, and optional 'flags' at the end, such as 'i' to indicate case insensitivity. So, **/cat/i** would match *cat*, *Cat* or *cAt*.

Many non-alphanumeric characters have special meaning, some of the most common are described below:

- . (period/full stop/dot) matches any character except a line break, so **c.t** will match *cat* or *cut*, but not *cant*.
- [...] matches any character defined inside the square brackets. Ranges can be specified using -, so valid ranges may be **[abc123]** or **[a-z0-7]**. So, **c[aeiou]t** will match *cat*, *cet*, *cit*, *cot* or *cut* but not *cbt*.
- \s means a space character (space, tab, line break)

- \ before any control characters (including \) means the second character literally rather than as a control character, eg * means *, not 'zero or more characters'
- * (asterisk/star) means zero or more of the preceding character, so **ca*t** will match *ct*, *cat* or *caaaaaaat*, but not *cbt*. The preceding character can be a control character or sequence as well, e.g. **c[a-c]*t**
- ? means zero or one of the preceding character or sequence, so **ca?t** will match *ct* or *cat*, but not *caat*.
- + means one or more of the preceding character or sequence, so **ca+t** will match *cat* or *caaaaaaat*, but not *ct*.
- {n,m} means from n to m of the preceding character or sequence, e.g. **c[aeiou]{3,5}t** will match *caaat*, *caiouat* but not *cat*, *caat* or *caeiouat*
- ^ is an "anchor" which matches at the start of a string
- \$ is an "anchor" which matches at the end of a string, so **/cat/** will match *cat*, *catch*, *abdicate*, but **/^cat/** will only match *cat* & *catch*, and **/^cat\$/** will only match *cat*.

There are many others.

For more details, or more examples, we recommend looking at a tutorial on the Internet.

6.8 SMTP MX Sending

When an end-user sends an email message, they will usually send it to an SMTP relay server (or 'smarthost'). This server will usually know about the sender, and may require them to use authentication to send messages.

The next step in sending the message is that the relay server has to send it to the recipient somehow. How it does that is done by using special DNS records called 'MX records'.

If you have an Internet domain, such as *mycompany.com* you will have DNS records associated with that domain. You may have an 'A record' associated with *mycompany.com* and *www.mycompany.com* so that web browsers know how to access the website at those names.

The DNS MX (Mail eXchange) record is a special type of record to tell other mail software where to send mail for your domain. So, the MX record may point to the name for your mail server - such as *mail.mycompany.com* (it has to point to a host name, not an IP address). You may have multiple MX records with the same or different 'priorities'. The sender should try the MX servers with lower priorities before trying those with higher priorities (if there are MX servers with the same priority, the sender can try them in any order it wishes).

This means that the MX records do not have to point to the same servers (or even servers run by the same company) as where the website is running, and do not have to be run by the same company as host your domain DNS records.

The process

So, if you are using MX sending, the sending software (eg VPOP3) will first look up the MX records for the domain being sent to. It will then try to connect to the servers contained in the MX records. It will try each one in order until it gets a response from one of them and then it will try to send the message through that server. (In some cases, the sender will not try further MX servers once it has received any response from one of them, in other cases, the sender will try all MX servers if it has received failure responses from previous servers. This is implementation dependent - there are advantages and disadvantages to both ways).

If the sending software does not receive a response from any of the MX servers or it receives a '4xx' response (meaning 'try again later') from all the responding servers, then it will hold the outgoing message in a queue to try again later. This means that if you have VPOP3 sending using MX sending, then you may see old messages in the OutQueue. That does not necessarily mean that VPOP3 has not tried to send the messages, but it could be that it has tried and failed to send it so far.

If the sending software does not receive a positive response after a short time (eg 4 hours) it will typically send a message back to the original sending user to say that the message has been delayed. If it does not receive a positive response after a longer time (eg 72 hours) it will fail the message, and send a delivery failure report back to the sender to say the message delivery attempt failed.

The long time before the message is failed is in case the receiving mail server is broken for a few days so that the administrators of that server have a reasonable chance to repair it without messages being lost.

If the sending software receives a 5xx response from an MX server it will typically fail the message immediately, because a 5xx response means that the message has not been accepted and delivery should not be reattempted.

If you are using an SMTP relay server/smarthost run by another company, then you will not see this retry behaviour occurring - you will just see the message being sent, and possibly delivery status notifications coming back. This does not mean the retry behaviour isn't happening, just that it is happening somewhere you can't see it.

6.9 Spamfilter

The VPOP3 spamfilter is a component which helps to reduce unwanted email messages (or 'spam').

The spam filter works by processing each incoming and outgoing message through a 'script'. The script assigns a 'score' to each message, and that score is used to determine whether the message is spam or not.

The [spam filter scripting language is documented on our wiki here](#). It is possible for administrators to create their own scripts for the spam filter to use. If you have a spamfilter subscription from us, then VPOP3 will periodically download updated script files to handle new spam attacks. These downloaded script files are encrypted, but VPOP3 will read plain text script files as well.

The scripts have many tests, such as:

- Checking for certain words & phrases in the message
- [Bayesian filtering](#)
- Checking for certain attachments or links
- Checking in user-defined white & blacklists

Because it uses a scripting language rather than a simple list of words & phrases to check for, it can perform more complex checks, such as 'check if the message asks you click a link to reset your password while claiming to be from a bank, but the link is not a link to that bank', and so on.

The tests are grouped into different 'rules', such as checking for phishing attacks, or adult material, or certain types of phrases etc. VPOP3 tracks what 'score' is given to each rule that is tested for, then it multiplies each rule's score by the 'weight' for that rule to calculate a final score. This weight mechanism lets administrators adjust the spam filter so that certain checks are given more or less importance depending on the situation. For instance, pharmaceutical companies may want to reduce the weight of the 'PossibleDrugs' rule because that will check for words like 'viagra' which are rarely seen in most users' legitimate messages, but may be quite common for a pharmaceutical company.

VPOP3 also has two different weights for each rule. The first is if the [Bayesian Filter](#) thinks the message is unlikely to be spam, and the second is if it thinks the message is likely to be spam. This allows some potentially benign checks to be given a higher ranking if the Bayesian Filter already thinks the message is spam.

The spam filter script writes the final score results to a message header called **X-VPOP3-Spam** as below

```
X-VPOP3-Spam: 65 - BulkMailer1(50.0) htmlonly(6.0) WebBug(9.0)
```

This header can be useful to diagnose what the spam filter is thinking. For instance, the above line indicates that the final score was 65 which is made up of scores from three rules - BulkMailer1, which had a score of 50; htmlonly, which had a score of 6, and WebBug, which had a score of 9.

If a message has a final score which is over a certain threshold (the default is 100), then it may be [quarantined](#) depending on the [global](#) and [user](#) settings.

It is possible for rule weights to be negative as well as positive - for instance, the 'whitelist' rule (which checks the sender address against a whitelist of known good senders) has a weight of -100, so that if a message's sender is in the whitelist it is almost impossible for the message to be marked as spam (unless the sender is also in the 'blacklist' which may cancel out or override the whitelist)

6.9.1 Quarantine

The VPOP3 Spamfilter Quarantine is a place where messages may be placed by the VPOP3 spam filter if they are deemed suspicious enough. The VPOP3 spam filter does not just delete messages because all spam filters have the risk of 'false positives' where legitimate messages are incorrectly detected as spam.

Each VPOP3 user has their own quarantine area where their suspicious messages are stored. Non-user entities (such as lists or forwarding email addresses) do not have a quarantine area so suspicious messages to those cannot be placed into a quarantine for that entity.

VPOP3 will hold the messages in the quarantine for a set time (default 14 days) and then automatically delete them. This time can be configured in the [Quarantine Settings](#).

Every day, VPOP3 will send a message to each user who has at least one message placed into the quarantine. This message will contain a summary of the quarantined messages, along with a link which can be used to view the message (and optionally release it for delivery). It is possible to alter the time when this summary message is generated, and even set VPOP3 to generate more than one a day. Again, this is set in the [Quarantine Settings](#).

Users can access their own quarantined messages at any time by logging into their Webmail account and selecting the 'Quarantine' tab.

Administrators can access the quarantined messages for any user by going to the [Settings -> Spamfilter -> Quarantine Viewer](#) page.

It is possible to disable the quarantine either globally (in [Settings -> Spamfilter -> General -> Quarantine settings](#)) or for an individual user (in [Edit User -> Advanced](#)). In this case, suspicious messages will be delivered to the user instead of placed into the quarantine.

6.9.2 Bayesian Filter

The Bayesian Filter is a component used by the [VPOP3 spam filter](#).

Bayesian filters are widely used in spam filtering - for instance, the spam filters built into many email clients use Bayesian filtering.

In the VPOP3 spam filter, messages are tested using the Bayesian filter, and the resulting rating affects the spam score using the **Bayes50**, **Bayes80**, **Bayes90** and **Bayes99** rules, depending on whether the Bayesian filter thinks the message was at least 50%, 80%, 90% or 99% likely to be spam.

The way a Bayesian filter works is quite complex and there are good articles on the Internet. One which made Bayesian filtering popular for spam filtering is by [Paul Graham](#), and Wikipedia has a [good article](#) on the subject. It is sometimes called a *naïve* Bayesian filter. The word 'naïve' is not a criticism of the method, just that it is a purely statistical approach without any attempt at being 'clever'.

Although a complete description is complex, the basic mechanism is explained below.

First the Bayesian filter is initialised with a set of data of both known good and bad email messages. How many times each word (or 'term') appears in good or bad messages is tracked, as well as how many good and bad messages in total there are. This data can be used to determine how 'spammy' a given word is likely to be.

For instance, our set of Bayesian data shows that the word 'replica' is found in 2.8% of spam, but only 0.1% of non-spam, so that means that the word can be calculated to be 'very spammy' because it is 28 times more likely to be found in spam than not spam.

There are less obvious examples, for instance a quick look through our Bayesian data shows that the word 'click' is found in about 30% of spam and 15% of non-spam, so it is twice as likely to be found in spam. On the other hand 'please' is in 34% of non-spam and 17% of spam, so twice as likely to be found in legitimate mail. The word 'can' is in 30% of non-spam and 19% of spam, so 50% more likely to be in legitimate mail, and so on.

When a message is received:

1. VPOP3 again breaks down the message into words and then looks to see how 'spammy' each word it finds is.
2. The VPOP3 Bayesian filter ignores any words it hasn't seen before at least 5 times (If it used rare words sooner then the results may be misleading).
3. Then, the Bayesian filter calculates how 'interesting' each word is. How interesting it is is determined by how far from '50% spammy' it is, for instance a word which is found in only spam or only non-spam is very interesting.
4. The Bayesian filter then throws away all words except for the 15 most 'interesting' words.
5. The filter then uses a formula to create an overall 'spamminess' value for the message based on the spamminess of these 15 most interesting words.

Because a Bayesian filter uses all the words (or 'terms') in a message it can sometimes be confusing. It does not work in the same way that a human would make the decision so it can seem a bit counter-intuitive. VPOP3 has a [page](#) where you can enter an email message and it will show details on the above steps to try to help you to understand how it works if you are interested.

As well as words in the message content, the VPOP3 Bayesian filter also processes message header data. In this case, it remembers it as '<header field>:<word>'. For instance the word 'viagra' in the message subject would be remembered as 'Subject:viagra'. This allows VPOP3 to also check for common sender addresses or even mail servers which are most often used for sending spam.

Training the Bayesian Filter

Bayesian filters need training with both good and bad messages so they can learn the probabilities of words being in either.

The VPOP3 Bayesian filter constantly trains itself using messages you manually mark as spam or not-spam. Also, if the VPOP3 spam filter detects a message is spam, it will train the Bayesian filter that it is spam, and if it doesn't detect it as spam or the message is sent by a local user, it will train the Bayesian filter that it is not-spam. This can lead to some reinforcement bias, but it makes it simpler for users to use. Otherwise there would have to be a strict regime of manually sorting out spam and not-spam and training the filter with significant amounts of each. If you want to turn off this self-training, then you can set the **UpdateBayes** value to '0' in the [script configuration settings](#).

You can also manually train the filter. If you send an unfiltered spam message to *spam@<your local domain>*, the spam filter will catch it and unlearn that it was good, and learn that it was bad. When you release a spam message from the [spam filter quarantine](#) or send it to *notspam@<your local domain>*, the spam filter will unlearn that it was bad, and learn that it was good.

Also, when users send messages to VPOP3 (either for local or external recipients), VPOP3 learns that that message is good (assuming that you don't send out spam).

6.10 Summary Log File Format

VPOP3 creates a file called SUMMARY.LOG in the VPOP3 directory which contains summary information which is compiled daily into a daily summary reports sent to the administrator.

VPOP3 can keep these summary logs in a subdirectory called SUMMARIES in case you want to do further processing on them. This article describes the format of the summary log files for you to use when parsing them.

Each line of the file is a separate record.

The line contains 4 elements

1. Date/time stamp
2. Item code
3. Value. In most cases this is a byte count
4. User name

The Date/time stamp is the date & time that this record was added.

The item code is one of

- 0 - Local email received
- 1 - Local email sent
- 2 - Internet email received
- 3 - Internet email sent
- 4 - System generated message received
- 5 - LAN Forward message queued (user name is sender)
- 6 - POP3 Client download
- 7 - SMTP Client send
- 8 - LAN Forward message sent
- 9 - Online Time (value is time in seconds)
- 10 - Urgent message sent
- 11 - LAN Forward message queued2 (user name is recipient)

So, if you want to see how much data was downloaded by the POP3 client component in VPOP3, scan through looking for lines where the item code is '6' and add all the values together.

6.11 VPOP3 Service Controller

The VPOP3 service controller is a small program which runs as a [Windows Service](#) and launches the main VPOP3.EXE program and database service (VPOP3DB).

The VPOP3 service program is called VPOP3SVC.EXE. As well as being the service controller, this program can also install and remove the VPOP3 service.

Command-line options

The VPOP3 service controller supports two commands

- QuickConfig - used to install the VPOP3 service
- QuickRemove - used to remove the VPOP3 service

QuickConfig

VPOP3SVC Quick Config is used to install the VPOP3 service

If you just run this alone, then the VPOP3 service will be created with the default options.

Other options are:

- **name=<name>** - Service Name used by Windows (defaults to 'VPOP3')
- **display=<display name>** - Service Display Name shown to user (defaults to 'VPOP3 Email Server'). If you set **name** and not **display**, then the display name is set to the service name.
- **inst=<instance name>** - Instance name to use (VPOP3 Enterprise only). Used for installing multiple copies of VPOP3 on the same PC
- **deps** - Configure service dependencies (dependency on VPOP3DB service) - not recommended

An example command line would be

```
vpop3svc quickconfig "name=My VPOP3" display=MyVPOP3Server inst=vpop3_2
```

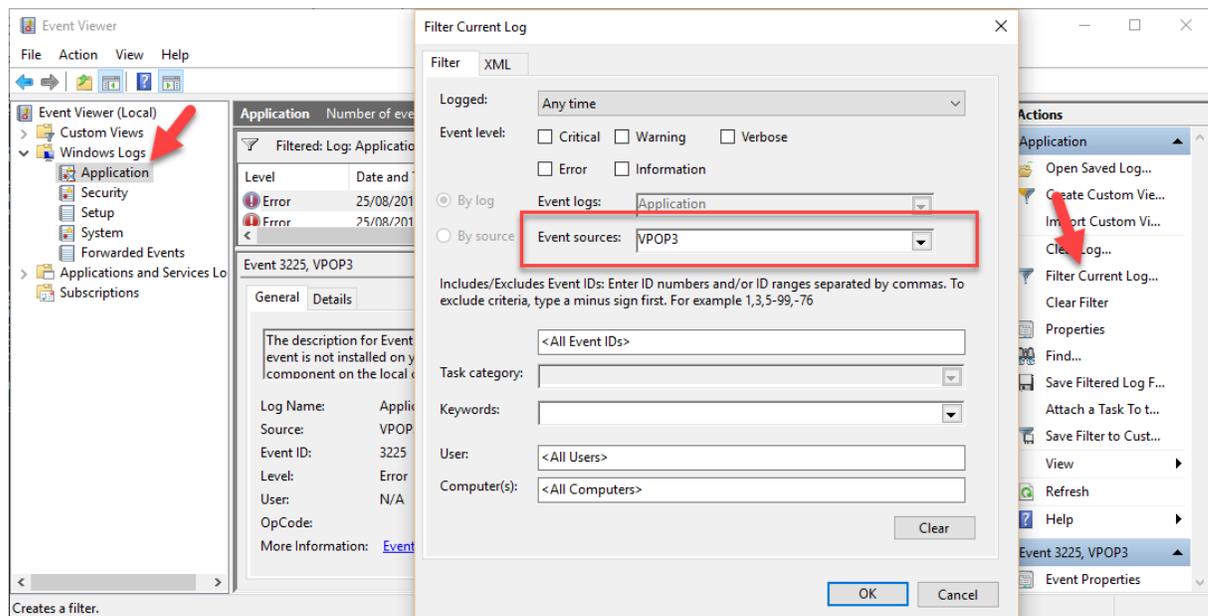
If you have VPOP3 Enterprise and want to install multiple VPOP3 servers on the same PC, you should specify at least unique values for 'name' and 'inst' on all installations (apart from, possibly, one of them, which can use the defaults).

QuickRemove

VPOP3SVC *QuickRemove* will remove the VPOP3 service. You can specify **name=<name>** to remove a specific instance if you installed it with a non-default service name.

Logging

The service controller writes key log information related to launching the VPOP3.EXE program to the Windows 'Application' Event Log which can be viewed through the Windows Event Viewer. The Application Name is 'VPOP3' so the filter option in the Event Viewer can be used to locate event log entries.



If the event log entries say: 'The description for Event ID xxx from source VPOP3 cannot be found' then it means that a message DLL has not been registered with the event viewer - see the [Event Log Problems](#) article for more help.

This service controller also writes basic log information to a file called *svc.log* in the same directory where VPOP3SVC.EXE is located. This log file is probably only useful for more detailed information on startup problems.

6.12 VPOP3 Status Monitor

The **VPOP3 Status Monitor** is a separate program which communicates with the VPOP3 server to have an easy-to-access way of viewing & accessing VPOP3.

The Status Monitor icon will usually appear in the Windows task tray (near the clock) as a British pillar postbox.

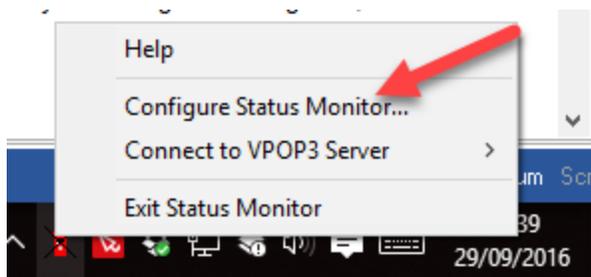


If the icon does not appear, it may be in the task tray overflow area. In Windows there is an up arrow to the left of the task tray. If you click on this, you will be shown the overflow area. You can customize which icons appear in the standard task tray by dragging them from the overflow area into the normal task tray. It can be very helpful to do this with the VPOP3 Status Monitor icon.

Configuring the Status Monitor

The VPOP3 Status Monitor has to be configured to connect to the VPOP3 server. That is because the Status Monitor can access VPOP3 across a network, and has to 'log into' the server so that VPOP3 knows what information and actions are available to the Status Monitor user.

To configure the Status Monitor, right-click the task tray icon to access the menu, then choose **Configure Status Monitor...**



If this option isn't available, you may need to **Disconnect from VPOP3 Server** first.

You will be shown a configuration dialog

Configure VPOP3 Monitor

The VPOP3 status monitor is a program which monitors the status of your VPOP3 server.
This program can be run on the VPOP3 computer itself, or on any other computer on the network.

Server Address: the IP address of your VPOP3 server
Server Port: usually 5109
User Name: the account name of a VPOP3 user (usually an administrator)
Password: the VPOP3 password of the account name specified in the "User Name" box

Server Name :

VPOP3 Server Address :

VPOP3 Server Port :

VPOP3 User Name :

VPOP3 Password :

Use Global Message Count instead of personal

Icon Colour :

IM Popup :

Allow 'Quick Exit' when connected

If you want to monitor multiple VPOP3 servers then you can create multiple Servers in the Status Monitor. To do this, choose **<New>** from the **Server Name** drop-down box and in the box underneath enter the name you want to use to refer to the new server. (To delete a server from the Status Monitor, select it, and press the **Del** button). To configure a different server, just select it from the **Server Name** drop-down box.

In the **VPOP3 Server Address** box, put the IP address or DNS name of the VPOP3 server you want to monitor

In the **VPOP3 Server Port** box, put the TCP port of the VPOP3 [Status Server](#). Note that this is usually **5109**. A common problem is that people think this is wrong, and "correct" it to 5108 because they are used to [accessing the VPOP3 settings](#) using port 5108. The Status Server does not use the Webmail/admin server, and is on a different port.

In the **VPOP3 User Name** and **VPOP3 Password** boxes, put the login details for a VPOP3 [User](#). You can put any user's details here depending on which person is going to be using the Status Monitor. If the **Only allow administrator access to status service** box is checked in the [Status Server settings](#), then only VPOP3 administrators will be able to use the Status Monitor. Different users may be able to access different functions and data using the Status Monitor, so if you can't see or do something you expect to be able to see or do, check the user's permissions in the [User's Permissions tab](#), or the [Status Server's Permissions tab](#).

If the **Use Global Message Count instead of personal** box is checked, then the Status Window and task tray icon will display the total Inbox message count for all users rather than the count for the logged in user.

The **Icon Colour** option lets you can change the colour of the icon. You can choose between the default red, blue, green, yellow, magenta, cyan and black. This can be useful if you have multiple instances of the Status Monitor connecting to multiple different servers.

The **IM Popup** option lets you decide whether a notification window will be displayed when a VPOP3 Instant Message arrives.

The **Allow 'Quick Exit' when connected** option lets you say whether you can exit the Status Monitor when it is connected to VPOP3 (usually you have to **Disconnect from VPOP3 Server** first, before you can **Exit**).

Using the Status Monitor

The Status Monitor has three main areas that are useful for monitoring & using VPOP3.

Icon

The Status Monitor icon itself will change shape depending on the status of VPOP3.

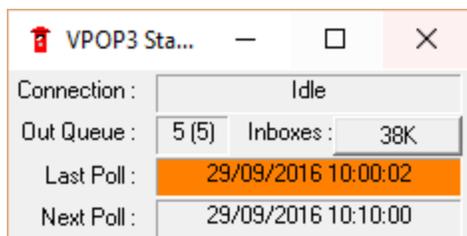
-  This is the normal icon. The VPOP3 Status Monitor is connected to VPOP3, and VPOP3 is idle (not actively sending or receiving messages), and there are no pending incoming or outgoing messages.
-  The VPOP3 Status Monitor is connected to VPOP3, and there are messages in the Inbox of the Status Monitor user.
-  The VPOP3 Status Monitor is connected to VPOP3, and there are messages waiting to be sent out from VPOP3.
-  The VPOP3 Status Monitor is connected to VPOP3 and VPOP3 is currently actively sending or receiving messages. There is a "flashing light" on top of the postbox.
-  The VPOP3 Status Monitor is not connected to VPOP3. This could be because VPOP3 is not running, or the Status Monitor can't log on for some reason.

The icon can show a combination of the above states depending on the state of VPOP3. For instance if there are messages in the user's Inbox, messages waiting to be sent out, and VPOP3 is currently collecting or sending mail, then the icon will be fat, have the letter going into the slot, and have a flashing light on top.

If you hover the cursor over the icon, then it will display a brief summary of the server name, VPOP3 licence name, total Inbox and Outqueue message counts as well as the logged in user's Inbox message count.

Status Window

If you double-click the VPOP3 icon in the task tray (or right-click it and choose **Status**) then the VPOP3 Status Window will be displayed.



This shows basic VPOP3 state:

- **Connection** - this shows the connection state of VPOP3. Idle, sending, receiving, etc. *Idle* means that VPOP3 is not currently actively collecting or sending messages, it does *not* mean that VPOP3 is not working or indicate a problem of any sort! If VPOP3 is currently sending or receiving, then this box will also display progress bars.
- **Out Queue** - this shows the number of messages waiting to be sent out. If there is a number in parentheses, then that number indicates the number of 'held' messages (which will not be sent as long as they are held). So, in the above example, there are 5 messages waiting to go out, and all 5 of those are held.
- **Inboxes** - this shows the number of messages in users' inboxes in VPOP3. This does *not* indicate the number of messages in an ISP's mailbox waiting for VPOP3 to collect. It indicates the number of messages in Inbox folders in VPOP3. Depending on how users' email clients are configured these messages may or may not have been read by the user. If there is a number in parentheses, then that number indicates the number of 'held' messages (which will not be visible to the user's email client as long as they are held). Depending on the [user's permissions](#), you may be able to click on the Inboxes value to see a list of all users with the number of messages in their Inboxes (at the expense of making VPOP3 work harder to keep the counts updated).
- **Last Poll** - this shows the last time VPOP3 tried to send or collect messages. If the background is red, then it indicates that, during that last poll, no action (collection or sending) succeeded. If it is orange, then it means that at least one action failed, and at least one succeeded.
- **Next Poll** - this indicates the next time that VPOP3 will try to send or collect messages.

Note that depending on the logged in [user's permissions](#), some or all of the above data may be blank.

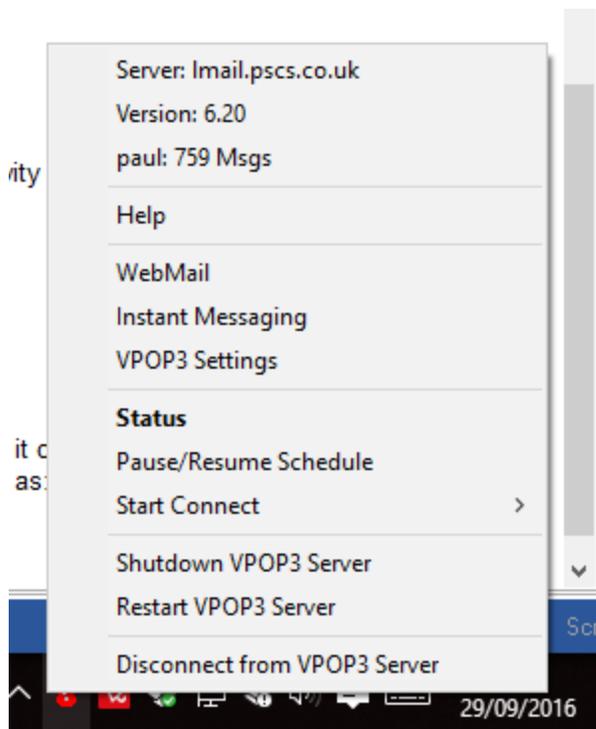
If you click on the VPOP3 icon at the left of the title bar, then the Windows menu will include a few extra options. You can also right-click anywhere in the top part of the Status window to see these options.

- **Always on top** - the Status Window will always be displayed on top of any other windows.
- **Show Activity Log** - the Status Window will expand to show an activity log below the basic status (this can also be done by double-clicking the title bar or 'maximising' the window).
- **Clear Activity Log** - this clears the activity log.
- **Copy Activity Log** - this copies the activity log contents to the Windows clipboard.

The Activity Log shows what VPOP3 is doing while it is sending or collecting messages. This can be useful to monitor activity. It does not show activity on the local network. If you right-click an activity log item, then a popup will appear, showing the timestamp of that item and the full details in case it was truncated in the Status Window.

Menu

If you right-click the VPOP3 icon in the task tray you will be shown a menu. The actual items in this menu may vary depending on the [permissions](#) of the user who is currently logged into the Status Monitor.



The top section of the menu are for display purposes only - the server name, version number and the number of messages in the logged-in user's Inbox.

Below that are more options depending on the user's permissions.

- **Help** - a link to the VPOP3 help.
- **WebMail** - a link to the VPOP3 Webmail.
- **Instant Messaging** - display a window allowing you to send simple instant messages to other VPOP3 users who are logged into the VPOP3 Status Monitor.
- **VPOP3 Settings** - a link to the [VPOP3 settings](#).
- **Status** - display the Status Window (see above).
- **Pause/Resume Schedule** - stop or restart VPOP3's automatic connections to send/receive messages. Pausing the schedule will stop VPOP3 collecting or sending any messages (incoming SMTP will still work).
- **Start Connect** - tell VPOP3 to start a connection to send & collect messages. If VPOP3 is currently connected, then this option changes to **Hangup Now** to tell VPOP3 to end the connection.
- **Shutdown VPOP3 Server** - stop the VPOP3 service
- **Restart VPOP3 Server** - restart the VPOP3 service
- **Disconnect from VPOP3 Server** - disconnect the Status Monitor from the VPOP3 Server.

If the Status Monitor is not currently connected to VPOP3, then the right-click menu will only allow you to reconfigure the Status Monitor or try to connect to VPOP3.

VPOP3 Status Monitor on other PCs

Because the VPOP3 Status Monitor connects to VPOP3 over the network, you can run it on any computer on your network. This can be useful if the VPOP3 server is not easily accessible because it can be run on the PC of the person who manages VPOP3. To use it on another user's PC, simply copy the **VPOP3STATUS.EXE** program onto the user's PC, then create a shortcut in the Windows startup group to that program, running it as:

```
vpop3status.exe /q /r
```

You can find the current user's personal Startup group by pressing Windows+R, then type **shell:startup** and press OK. Then right-click and choose **New -> Shortcut** to create the startup item.

6.13 VPOP3.INI format

The VPOP3.INI file is a file in the VPOP3 installation directory. It primarily contains configuration details so that VPOP3 knows how to contact the PostgreSQL database server where the majority of the VPOP3 settings are stored. Obviously VPOP3 can't use settings in the database to tell it how to connect to the database.

The VPOP3.INI file also contains some other settings which may be needed in the early stages of program start, or which need to be inaccessible from the database.

The INI file uses the [standard INI file format](#).

(We know that Microsoft recommend using the registry for settings rather than INI files, but we have found it easier for people to maintain INI files than the Windows registry).

VPOP3 needs to be restarted after any settings in this file are changed.

Database Configuration

The database configuration is in a INI file section called 'database'. An example is below

```
[Database]
Database=vpop3
User=vpop3
Password=vpop3pass
Hostname=localhost
Hostaddr=
Port=5433
Timeout=0
Options=
SSLMode=prefer
Service=
MaxConnections=30
AbsMaxConnections=50
```

- **Database** is the PostgreSQL database name for the VPOP3 settings. Usually this is 'vpop3'.
- **User** is the PostgreSQL login name to access the above Database. Usually this is 'vpop3'.
- **Password** is the password for the above User. Usually this is 'vpop3pass'
- **Hostname** is the host *name* used to access the database server. This has to be a DNS name. Usually this is **localhost** because PostgreSQL is installed on the same PC as VPOP3 (but this does *not* always need to be the case)
- **Hostaddr** is the host IP address used to access the database server. This has to be an IPv4 or IPv6 address. One of Hostaddr or Hostname needs to be set. Usually this is blank so the **hostname** is used, but you could use **127.0.0.1** or **::1** here to refer to the same PC as VPOP3 if you wish.

- **Port** is the TCP port used to connect to the PostgreSQL service. The VPOP3 installer finds the first free port after 5432 (the default PostgreSQL port) to use. Usually this is **5433**.
- **Timeout** is the connection timeout (in seconds) for connecting to PostgreSQL. Usually this is **0** meaning no timeout.
- **Options** allows you to set command-line options to send to the PostgreSQL server. Usually this is blank.
- **SSLMode** indicates whether secure SSL is to be used to connect to the PostgreSQL server. The options are **disable**, **allow**, **prefer**, **require**, **verify-ca** and **verify-full**. If it is blank, then **prefer** is used. See the [PostgreSQL documentation](#) for more details.
- **Service** indicates the PostgreSQL service to use. Usually this is left blank. Other options are not supported by us, but if you must use them, you option's here, but you're on your own.
- **Max Connections** indicates the maximum number of normal connections to the PostgreSQL server that can be in the connection pool.
- **AbsMaxConnections** indicates the absolute maximum number of connections if VPOP3 has to make extra connections due to pool exhaustion.

Extra configuration

There are two types of extra options: those which have to apply early in the VPOP3 load cycle, and those which need to be inaccessible from within VPOP3.

Early options

```
ShowSplashScreen=1
LogWriterWaitThreshold=1000
```

ShowSplashScreen indicates whether the VPOP3 splashscreen should be shown when VPOP3 starts as a normal application (when launching VPOP3.EXE directly, rather than as a service). It can be '0' or '1'. We recommend it is set to '1'

LogWriterWaitThreshold is a limit used to slow VPOP3 down if the disk is behaving too slowly to accept log entries. VPOP3 will wait 1 ms for each <LogWriterWaitThreshold> lines waiting to be written to the log files. If this is over 10ms, then VPOP3 will purge the log file entry queues and wait until that purge has finished. The default is 1000

Hidden options

These options can be used if VPOP3 is installed on your servers for use by someone else. Because VPOP3 administrators cannot access the VPOP3.INI file through the VPOP3 settings, it allows you to configure some things that cannot be changed by the VPOP3 administrators. Obviously if the VPOP3 administrators have access to the server disk, they can edit this file, so the usefulness of these settings is minimal in that case.

```
UserRestriction=27
LockBindings=192.168.3.2
HideLicence=1
LockDBQuery=1
SafeAttachExtract=1
HideSSLCertificate=1
```

UserRestriction lets you set the licenced user size to lower than the actual licence size. For instance, you may be running a hosted copy of VPOP3 for someone else, but they just want 20 users. A VPOP3 licence is not available for 20 users, so you could buy a 25 user licence, and set **UserRestriction=20**. VPOP3 will then restrict itself to 20 users. If you set this higher than the real licence size, then this setting is ignored.

LockBindings lets you restrict [service binding](#) editing by the user. If this is set to 0 (or not present) then the service bindings can be edited as normal. If it is set to '1' then bindings cannot be edited at all. If it is set to an IP address (in v6.20 or later) then bindings can be edited, but only the specified IP address is available, instead of all IP addresses on this computer.

HideLicence lets you specify that the VPOP3 licence details cannot be viewed or edited on the [About](#) page.

LockDBQuery lets you specify that the **Database** -> [Query](#) page is inaccessible. This prevents an administrator from messing with things at a low level (eg to alter bindings or licence details by accessing the settings database table)

SafeAttachExtract lets you specify that attachment extraction can only be performed to subdirectories of the main VPOP3 installation directory, regardless of the VPOP3 settings.

HideSSLCertificate lets you restrict access to the SSL certificate configured into VPOP3 through the settings. For instance, if it is a shared certificate where you don't want someone else to be access the private key. (In 7.1 and later)

6.14 Wildcards

VPOP3 supports *wildcards* in many places. These are similar to the * and ? wildcard characters using in DOS and Linux.

In VPOP3 a * matches zero or more of any character, and ? matches exactly any one character.

So, **ca*er** will match *caterpillar*, *caper*, *caer*, etc and **ca?er** will match *caper*, *cater* but not *camper* or *caer*.

In VPOP3, you can use multiple wildcards in one string, eg **ca*er*ly** will match *caerphilly* and *caleraply* and *camdfewfqqwfergewgehasdly*.

DOS wildcards don't always work well with multiple wildcards in one string.

7 Trouble Shooting

7.1 BCC Messages and catch-all POP3 mailboxes

When VPOP3 is configured to download mail from a shared (catch-all) [POP3](#) mailbox at your ISP, it has to read through the standard message header lines to see who the message is for. It looks at the To, Cc, Received, Apparently-To, Resent-To and Resent-Cc header fields for a recipient it recognises.

In most cases this will work fine. However, if the message has been BCCd to you, the recipient address will not be in the message header at all (that is the whole point of BCCd mail). The message reaches your ISP mailbox because the actual recipient is listed in the [SMTP Envelope](#) but most ISPs will throw that information away when they deliver the message into a POP3 mailbox. Because of this there is no automatic way that VPOP3 can work out the message's recipient(s). Instead it will deliver the message to the failed recipient address specified in the [Mail Collector](#) → [Routing Errors](#) settings in VPOP3.

Possible Solutions

Some ISPs will copy the SMTP Envelope recipient information into custom header fields in the message, such as **X-RCPT-TO** or **Delivered-To**. In this case, you can tell VPOP3 to use this header information (see the **Custom Headers** section below).

If your ISP does not copy the SMTP Envelope information into the header your options are limited:

- **Manually.** An administrator can go through the messages which were not delivered, and forward them to the appropriate person.
- **Mappings.** Many BCCd messages are actually from mailing lists. In this case the **To** header will often have the address of the mailing list in it. In this case you can create a **Mapping** of type **POP3** from the mailing list address to the user(s) who want to receive the message.
- **SMTP Feed.** If you can switch to an incoming SMTP Feed for your mail (instead of POP3 collection), then that will allow the SMTP Envelope information to be given directly to VPOP3, so the problem will vanish. This is the recommended option if it is possible for you.
- **Individual POP3 mailboxes.** If your ISP uses its SMTP feed to sort the messages into individual POP3 mailboxes at the ISP, then VPOP3 can download the messages from those and use which mailbox the message was in to determine which local user should get the message. The BCC problem only applies to shared POP3 mailboxes, not to individual POP3 mailboxes.

Custom Headers

If your ISP adds custom header information, then, to tell VPOP3 about this, go to [Mail Collectors](#) → [POP3 Routing](#) → [Configure Routing Options](#) in the VPOP3 settings. In the **Special Header Fields** box put information defining the header field(s) which you want VPOP3 to look at. Some examples are:

- **Delivered-To:** - Finds *user@domain.com* in *Delivered-To: user@domain.com*
- **X-RCPT-To:** * - Finds *user@domain.com* in *X-RCPT-To: user@domain.com* (equivalent to the above one)
- **Delivered-To:** 547-* - Finds *user@domain.com* in *Delivered-To: 547-user@domain.com* (specifies an explicit prefix)
- **Delivered-To:** 547-* confirmed - Finds *user@domain.com* in *Delivered-To: 547-user@domain.com confirmed* (specifies an explicit prefix & suffix)
- **Delivered-To:** 547-* ~ - Finds *user@domain.com* in *Delivered-To: 547-user@domain.com random text* (specifies an explicit prefix and random suffix)

7.2 Event Log Problems

A common problem with the Windows Event Log is when a required message DLL is not registered with the event viewer. This can happen with other software as well as VPOP3.

If this has happened, then when you view an event in the Event Viewer it will say: **The description for Event ID xxxx from source yyyy cannot be found**

Because the Event Viewer cannot possibly know about all the possible event messages from all possible programs, each program which writes to the event log has to register a 'message DLL' with the event viewer. This DLL contains the message IDs and text.

For VPOP3, this DLL is called 'vpop3msg.dll' in the VPOP3 installation directory.

For PostgreSQL, this DLL is called 'pgevent.dll' in the VPOP3\pgsql\lib directory.

Manually register the VPOP3 message DLL

1. To manually register the VPOP3
2. Run the Windows Registry Editor REGEDIT.EXE
3. In the left pane, find
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application
4. Right-click **Application** in the left pane, and choose **New > Key** and create a new key called **VPOP3**
5. In this new Key, in the right pane:
 - a. Choose **New > DWORD (32 bit) Value** and create a new Value **Category Count** with value **2**
 - b. Choose **New > DWORD (32 bit) Value** and create a new Value **Types Supported** with value **7**
 - c. Choose **New > String Value** and create a new Value **CategoryMessageFile** with value **c:\vpop3\vpop3msg.dll** (or wherever the vpop3msg.dll file is located)
 - d. Choose **New > String Value** and create a new Value **EventMessageFile** with value **c:\vpop3\vpop3msg.dll** (or wherever the vpop3msg.dll file is located)

Name	Type	Data
(Default)	REG_SZ	(value not set)
CategoryCount	REG_DWORD	0x00000002 (2)
CategoryMessa...	REG_SZ	H:\vpop3\vpop3msg.dll
EventMessageFile	REG_SZ	H:\vpop3\vpop3msg.dll
TypesSupported	REG_DWORD	0x00000007 (7)

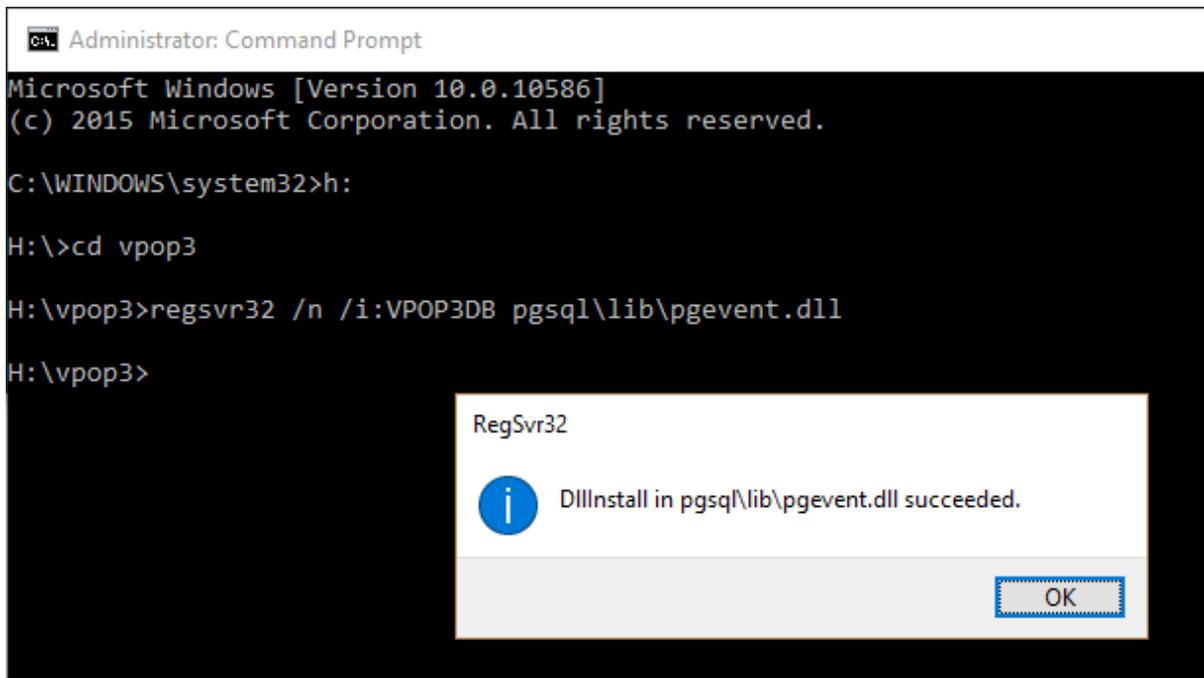
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\VPOP3

Restart the Event Viewer if necessary.

Manually register the PostgreSQL message DLL

Launch a command prompt as an administrator and navigate to the VPOP3 folder

run: `regsvr32 /n /i:VPOP3DB pgsqllib\pgevent.dll`



Restart the Event Viewer if necessary.

7.3 Troubleshooting login problems

There are several reasons that people have problems logging into VPOP3's services.

The most important diagnostic tool for troubleshooting these problems is the SECURITY.LOG file which is stored in the VPOP3 logging folder on disk. It can also be accessed in [Settings -> Diagnostics](#) by pressing the **View SECURITY.LOG** button. The SECURITY.LOG file will contain more information than errors returned to the user, because the errors returned are deliberately generic to avoid giving information to an attacker - for instance, if you tell an attacker that a username is unknown, it tells them they should try another username instead of attempting another password.

Incorrect login details

The most common, by far, is that they are using incorrect login details - ie an incorrect username or password. (The username is sometimes called the login name, or account name or similar).

The **username** is the name specified in the [Users](#) list in VPOP3. It is *not* the email address or a 'similar' name. So, if the name in the **Users** list is "robert", using "robert@mycompany.com" or "bob" will not work! Usernames are not case sensitive.

The password is exactly the password specified for the user in VPOP3. Passwords *are* case sensitive.

Incorrect Access Restrictions

Each VPOP3 service has [Access Restrictions](#) which tell VPOP3 which users can access the service from which IP addresses. Make sure these are set correctly.

Incorrect Permissions

Each VPOP3 user has [permissions](#) which allow them to use certain VPOP3 services, for instance users could have their SMTP service access blocked in their user settings.

Index

- * -

*REMOTE 167

- . -

.LUA files 444

- 4 -

450 4.7.1 Recipient Prohibited 226

450 4.7.1 Sender Prohibited 226

454 4.7.1 Message Prohibited 226

- 5 -

550 5.7.1 Mail not allowed because client address
A.B.C.D found in RBL entry 237

550 5.7.1 Recipient Prohibited 226

550 5.7.1 Sender Prohibited 226

554 5.7.1 Message Prohibited 226

- A -

Accepted domains 188

Access blocked temporarily 394

Access Restrictions 269

 GeolP 271

 IMAP4 249

Access temporarily blocked 394

Account expires at end 97

Account Lock 392

Account locked out 97

Account Lockout Policy 392

Accounts

 Adding 94

 Deleting 131

 Editing 96

 Grey 97

 Greyed 94

Active Directory 392

Add a Mail Collector 176

Add Date: header field to locally sent messages if it
doesn't exist 241

Add original recipients to custom header if message
delivered to local mailbox 241

Add Users 94, 141

Address Book

 Link to external database 256

Address Book from external database 255

Address book in Webmail 103

Administrator 59, 97

Admins 167

ADSL 170

Advanced 125

Advanced Routing Options 190

Aliases 74, 118, 167

Allow Any Line Endings 383

Allow LAN Forwarding addresses without a specific
domain 352

Allow list members to request a list of members from
the ListServer 159, 165

Allow modification of Global Address Book by users
254

Allow people to subscribe to the list themselves 158

Allow receiving of Internet mail 115

Allow Remote Access 79

Allow Remote Administration 159, 165

Allow sending BCCs 115

Allow sending of Internet mail 115

Allow user to access message archive 103

Allow user to change autoresponder via Webmail
103

Allow user to change forwards/assistants via Webmail
103

Allow user to change names of special folders in
Webmail 103

Allow user to change their Real Name setting in
Webmail 103

Allow user to create calendars in Webmail 103

Allow user to see global address book entries 103

Allow user to share calendars in Webmail 103

Allow user to view images in Webmail 103

Allow users to log in using their Windows passwords
392

Allow viewing of quarantined messages without logging
in 397

Allow ZIP file to be bigger than target size 369

Allowed Protocols 115

Apply account lockout policy to WebMail/Admin even
when connecting from 127.0.0.1 392

Archive 361

Archive Backup Location 369
 Archive Backup Name 369
 Archive Main Store 361
 Archive Messages 361
 Archive messages to this list 159, 165
 Archive Offline Backup 369
 Archive search results 368
 Archived Messages 103, 360
 Assistant 100
 Associate email address to user 118, 167
 ATRN 64
 ATRN Collection 176, 177
 ATRN Mail Collection 179
 Attempt to work with a single email address 188
 Authentication ID 372
 Authentication Method 200
 Authentication-Results header 372
 Autodetect proxy settings if possible 382
 Automatically block IP addresses 244
 Automatically deleting messages 128, 311
 Autoresponder
 Definitions 105, 108
 Filters 105
 Header filters 302
 Lua 108
 Reply filters 302
 Rule 113
 Rules 105
 Scripts 108
 Templates 108, 302
 Triggers 105
 Auto-submitted header 302

- B -

Backscatter 355, 373
 Backup 11
 Local Backup 305
 Offsite Backup 323
 Restoring 91
 To Amazon S3 314
 Backup Command Options 305
 Backup Command Sample 305
 Backup database now 305
 Backup Target File 305
 Bad Authentication Multiplier 244
 Bad Local Rcpt Multiplier 244
 Bandwidth pools 388

Bandwidth throttling 274, 388
 bandwidth.lua 274
 Bang email address 241
 Basic Edition 59
 BATV 373
 BATV Secret 373
 Bayes Filter 399, 454
 Bayesian Analysis 399, 454
 Bayesian Database 399, 454
 Bayesian Spamfilter 399, 454
 BCC 241
 BCCs
 Restrict sending 115
 Biggest Folders 311
 Blackhole SMTP messages 226
 Blacklist 452
 Blank From address 207
 Blank return paths 207
 Block IP addresses 226
 Block List 244
 Block outgoing messages if over X messages in the Outqueue 241
 Block outgoing messages if over X messages in the Outqueue from this user 241
 Block receiving from particular address 115, 226
 Block sending to particular address 115, 226
 Bounce Address Tag Validation 373
 Buffer logging data 325
 Bulk Add Users 141
 Bulk delete outgoing messages 134
 By default return all available attributes 255

- C -

Cable 170
 Cache Windows passwords 392
 CalDAV 59
 Calendars
 Creating 103
 Sharing 103
 Call Forward Verification 355
 catch-all mailbox 188
 Change Internet Mail Reply Address To 125
 Change NULL return paths to 207
 CIDR 436
 Clear all users' individual quarantine thresholds 397
 Clear Bayesian Statistics 399
 Client Error Block Threshold 244

Client Error Block Time 244
 Client Error Monitor Period 244
 Client Error Re-Block value 244
 Collector
 SMTP 195
 Column Titles 140
 Command to run after backup 305
 Concurrent FETCHes for a user 249
 Concurrent FETCHes for this server 249
 Concurrent logins for a user 249
 Concurrent logins from an IP address 249
 Concurrent SEARCHes for a user 249
 Configure Routing Options 188
 Configure Status Monitor 458
 Connect email address to user 118, 167
 Connect through SOCKS proxy Server 175
 Connection 170, 172, 173
 Adding 171
 Advanced Settings 175
 Copy Messages 100
 Copy messages to folder 119
 Copy Sent Messages To 100
 Custom Headers 190
 Custom unsubscribe message 158
 Custom welcome message 158

- D -

Daily Quarantine Report Recipient 125
 Database 304, 311
 Database address book 255
 Database backup successful email messages 305
 Database backups 305
 Database link for LDAP 255
 Database Restore 320
 DBBACK files 305
 Default Connection 173
 Default Quarantine threshold 397
 Delay when moving messages 311
 Delete a Mail Collector 176
 Delete messages from the quarantine after x days 397
 Delete POP3 messages 183
 Delete User 131
 Deleted outgoing messages after 125
 Deleting messages automatically 128, 311
 Delivery Status Notifications 241
 Diagnose message misdelivery 333

Diagnosing login problems 469
 Diagnostics 325
 Outgoing Mail 132
 Dial-in server 81
 Dial-up 170, 173, 195
 Dial-up connections which can also be used for this connection method if already established 175
 Direct MX Sending 198
 Disable DSN 241
 Disable links in messages 103
 Disclaimer 123, 124, 339, 445
 Disk Caching 11
 Disk Space checking 380
 Distribution List 149
 Distribution Lists 72
 DNS Blacklists 237
 DNS Cache Size 203
 DNS MX Record 89
 DNS Overrides 203, 204
 DNS Servers 203
 DNSBL 237
 DNSBL Match Multiplier 244
 Domain Filtering 210
 Don't add a signature with messages from this account 123, 124
 Don't allow addresses with '!' in their address 241
 Don't allow addresses with '%' in their address 241
 Don't archive Spam 361
 Don't multi-thread VPOP3 Plugins 383
 Don't route local mail locally 383
 Don't use forwardings or assistants if mail would be quarantined 100
 Download from a POP3 Server 179
 Download Rules 183

- E -

Edit a Mail Collector 176
 Edit DNS Overrides 203
 Edit SMTP Rules 225
 Edit User 96, 145
 Editions
 Basic 59
 Enterprise 59
 Home User 59
 eM Client 37
 Email Address to User mapping 118, 167
 Email Addresses 103

Email client configuration 24
Email Footer 445
Email loops 207
Email Protocols 60
Email Service Provider 70
Email Signature 445
EML files 130, 443
Empty folders 130
Empty From address 207
Empty return path 207
Enable BATV Support 373
Enable daily database backups 305
Enable disk space checking 380
Enable IDS Logging 244
Enable Minger server on UDP port 4069 241
Enable Quarantine Facility 397
encrypt 66
encryption 66
Enter licence details 433
Enterprise Edition 59
Error Message
 450 4.7.1 Recipient Prohibited 226
 450 4.7.1 Sender Prohibited 226
 454 4.7.1 Message Prohibited 226
 550 5.7.1 Recipient Prohibited 226
 550 5.7.1 Sender Prohibited 226
 554 5.7.1 Message Prohibited 226
 Too many concurrent searches - try again later
 249
 Too many connections from this address! 249
 Too many current FETCHes active 249
 Too many hops 383
 Too many logins for this user 249
Errors logging in 469
Errors Only 325
Errors.log 325
ESP 70
ETRN 64, 195
Event Logs 456
Everyone 115, 167
Export messages to EML or MBOX files 130
Export users to file 140
External Database Mailing List 162
External Fax software 381
External Router 347
Extra Archive Actions 361

- F -

Failed login block time 392, 394
Failed login threshold 392, 394
Failed logins 325
Fake access to inaccessible mailboxes 249
Fax
 Third party software integration 381
Files 443
Filter boxes 92
Filter Message 226
Filter SMTP messages 226
Filtered Attachment Multiplier 244
Filtering Mail 183
Filtering messages 119
Filtering outgoing messages 210
Filtering SMTP messages 447
Finger Service 252
 Access Restrictions 253
 Info 253
 Plan 253
 Template 253
Firewall 89
Folder permissions 130
Folders
 Copy 130
 Delete 130
 Empty 130
 Move 130
 Prevent deleting, renaming or moving 130
 Rename 130
Folders - Biggest 311
Footer 123, 124, 339, 445
Forward all messages to another LAN mail server
using SMTP 188
Forward messages 119
Forward To 100
Forwarding messages to another SMTP Server 352
Free memory checking 380
Full Logging 325

- G -

Gateway Servers 372
Generate digest messages every X days 159, 165
Generate quarantine report now for 397

GeolP restrictions 271
 GetInternalSignature function 445
 GetSignature function 445
 Global Address Book 67
 Modification by Users 254
 Global Prune Rules 311
 Global Sender Blacklist 379
 Global Sender Whitelist 379
 Global Signature 339
 Global Signatures 123, 124
 Global Target Blacklist 379
 Global Target Whitelist 379
 Good Local Rcpt Multiplier 244
 Greyed user 94, 97
 Grids 92
 Groups 167

- H -

Header Processing 190
 Headers
 Authentication-Results 372
 X-RBLFound 237
 X-VPOP3-ORIGRCPT 241
 Hold Obsolete UIDLs for X days 383
 Hold outgoing messages for 125
 Host Name 241
 HTTP Proxy 382
 HTTP Proxy Settings 382

- I -

IDS 244, 445
 IDS Log Filename 244
 IDS Log Line Format 244
 IDS.LOG 445
 If this connection fails totally, try another Connection 175
 Ignore POP3 messages 183
 Ignore SMTP messages 226
 IMAP4 59, 60, 65
 IMAP4 access restrictions 249
 IMAP4 Server 249
 IMAP4rev1 Server access not allowed 249
 Immediately copy messages already in this user's
 Inbox to assistant(s) 100
 Import GeolP data 271
 Import Users from file 136

Import Users from Windows users 139
 Inactive user 97
 Include Passwords 140
 Incoming connections 81
 Incoming SMTP 89, 176, 177, 195
 Incoming SMTP Mail Feed 179
 Inform the list moderators of any new subscriptions or
 unsubscriptions 158
 Inform the list moderators of any unsubscriptions
 158
 In-reply-to header 302
 Install VPOP3 service 456
 Instant Messaging 458
 Internal Signatures 124
 Internet Mail Access Protocol v4 60, 65
 Internet Service Provider 70
 Intrusion Detection System 244, 445
 Intrusion Prevention 394
 Intrusion Protection 392, 394
 Intrusion Protection System 244
 IP Access Restrictions 269
 IP Address 85
 IP address blocked 394
 IP addressing 436
 IP routing 436
 IPS 244
 ISP 70

- K -

Keep archive messages for X days 159, 165
 Keep Internal Date and Message Flags when
 messages are copied 249

- L -

LAN Forwarding 352
 LAN Forwarding Queue 357
 LAN Forwarding verification 355
 LDAP 67, 255, 256
 LDAP Service 254
 Access Restrictions 255
 Legacy Extensions 347
 Licence 76
 details 433
 entering 433
 key 433
 viewing 433

- Limiting access to VPOP3 services 269
 - Limiting bandwidth 274, 388
 - Link email address to user 118, 167
 - Links not working in quarantine reports 397
 - List 149, 153, 162
 - List Digests 159, 165
 - List Moderator 159, 165
 - Listening ports 273
 - Lists 167
 - Listserver for this list 158
 - List-Unsubscribe header 156, 164
 - Local mail
 - Allow only local mail 115
 - Lock user after x invalid login attempts 392
 - Lock user for x minutes 392
 - Log Files 325
 - SECURITY.LOG 469
 - Log Level 325
 - Log Path 325
 - Log Rejected unrecognised recipients 241
 - Logging 325
 - Login failures 325
 - Login problems 469
 - Lua 391, 444
 - Lua Functions
 - GetInternalSignature 445
 - GetSignature 445
 - ProcessLine 445
 - Lua Script
 - Bandwidth throttling 274
 - Editing 391
 - IDS Logging 445
 - Management 391
 - Signature 445
 - SMTP Server 237
- M -
- Mail Collector 176, 177
 - Method 179
 - Name 179
 - Priority 179
 - Mail Collector Method 177
 - Mail Collector Name 177
 - MAIL FROM 207
 - Mail loops 207
 - Mail Sender 197, 198, 200
 - Mailbox Quota 426
 - Mailer Daemon Name 383
 - Mailing List 72, 153
 - Confidential 158
 - Digests 159, 165
 - External Database 162
 - Header modifiers 156, 164
 - Headers 156, 164
 - List-Unsubscribe header 156, 164
 - Moderators 159, 165
 - ODBC 162
 - Remote Administration 159, 165
 - Reply to list 156, 164
 - Return Address 159, 165
 - Signature 156, 164
 - Spam 159, 165
 - Stop read receipts being generated 156, 164
 - Subscriptions 158
 - Unsubscribe Message 158
 - Unsubscriptions 158
 - Use To instead of Bcc 159, 165
 - Verify Subscriptions 158
 - Welcome Message 158
 - Main Administrator 131
 - Main Archive Store Directory 361
 - Make autoresponders conform to RFC 3834 302
 - Manage block list 244, 392, 394
 - Manage never block list 244, 392, 394
 - Managed Service Provider 70
 - Mappings 74, 118, 167
 - Mark as not-spam 454
 - Mark as spam 454
 - Mass delete outgoing messages 134
 - Max failed login attempts 241, 249
 - Max Hops 383
 - Max Messages per Session 202
 - Max outgoing message size 115
 - Max Recipients per Message 202
 - Max Recipients per Session 202
 - Maximum line length 241
 - Maximum log size 325
 - Maximum number of LAN Forwarding threads 352
 - MBOX files 130, 443
 - Memory checking 380
 - Message Archive 103, 360
 - Compress 362
 - Configuration 361
 - Copy 362
 - Encrypt 362

Message Archive 103, 360
 Extra Actions 362
 FTP 362
 Move 361, 371
 Moving to ZIP file 369
 Rescan 371
 Retrieve messages 368
 Search 367
 Search results 368
 SFTP 362
 Message Misdelivery 333
 Message Prohibited error message 226
 Message Recovery 125
 Message Recycle Bin 311
 Message Recycle Bin Size 125
 Message Restore 320
 Message routing 100, 188
 Message rules 119
 Message Store 311
 Message Store Stats 311
 Message To Big Multiplier 244
 Messages
 Outgoing 132, 134
 Messages Received Report 422
 Messages Sent Report 423
 Messages Summary Report 424
 Messaging VPOP3 users as administrator 144
 Microsoft Outlook 2016 configuration 43
 Minger 241, 355
 Minger Secret 241
 Minimum Password Length 392
 Mirroring VPOP3 314
 Modem 81
 Monitor logins period 392, 394
 Monitor Messages 115
 Move folders to another user 130
 Move messages to folder 119
 MSG files 443
 MSP 70
 Multiple VPOP3 servers 314
 MX Record 89
 MX Record overrides 204
 MX Sending 198, 203, 451
 MX sending threads 203

- N -

Never Block List 244

No-one 167
 Notepad++ 444
 NT Passwords 392
 NULL Characters in POP3 downloads 383
 Null return paths 207

- O -

ODBC 256
 ODBC Mailing List 162
 ODMR 64
 ODMR Collection 176, 177
 ODMR Mail Collection 179
 Offline Archive Backups 369
 Offsite Backup 323
 On Webmail quarantine release, add to whitelist 103
 On Webmail quarantine release, report false positive 103
 On Webmail quarantine release, train Bayesian filter 103
 Only collect addresses if user has logged into Webmail within last X days 241
 Only collect mail addresses for users who have Webmail permission 241
 Outgoing Mail 197
 Delete 132, 134
 Hold 132, 134
 Outgoing mail priority 125
 Outgoing Message Queue 92
 Outgoing Signatures 123
 Outlook 2016 configuration 43
 Outmail Pre-Processor 347
 Out-of-Office Reply 105, 302
 Outqueue
 Bulk Actions 134
 Delete 132, 134
 Hold 132, 134
 Retry 132, 134
 View 132

- P -

Parameters for ETRN 195
 Partial Attachment Multiplier 244
 Password Length 392
 Passwords 98
 Percent hack 241

- pg_dump 305
- Plugins 347
- Polled SMTP 177
- POP3 59, 60
- POP3 Collection 176
- POP3 Download 177
- POP3 Filtering Rules 183
- POP3 routing options 188
- Port 25 200
- Port 465 200
- Port 587 200
- Port Forwarding 89
- Ports 200
- Post Office Protocol v3 60
- Post-Connect Command 347
- PostgreSQL 304
- PostgreSQL Binary Directory 305
- Precedence header 302
- Precedence header for autoresponses 302
- Pre-Disconnect Command 347
- Prevent user receiving incoming mail 115
- Prevent user sending outgoing mail 115
- ProcessLine function 445
- Prohibit receiving from particular address 115, 226
- Prohibit sending to particular address 115, 226
- Protocols
 - Email 60
 - IMAP4 60, 65
 - POP3 60
 - SMTP 60, 62
- Proxy 382
- Proxy Server 175
- Proxy server address 382
- Proxy server port 382
- Prune Rules 128, 311
- prvs= address prefix 373
- Put user in Everyone list 115

- Q -

- Quarantine daily reports 397
- Quarantine Report 125
- Quarantine report schedule 397
- Quarantine server address 397
- Quarantine Threshold 125
- Query Download Delay - X days 383
- quickconfig 456
- quickremove 456

- Quotas 426

- R -

- RAMDisk 325
- RBL 237
- Realtime Blacklists 237
- Received Message Report 422
- Recipient Prohibited error message 226
- Recover deleted emails 125
- Recycle Bin 125, 311
- Recycle Bin Size 311
- Redirect mail 167
- Redirect POP3 messages 183
- Redirect SMTP messages 226
- Redirect Spam 401
- Redirect to Assistant 100
- References header 302
- Refuse SMTP Connections from 241
- Reject POP3 messages 183
- Reject SMTP messages 226
- Relay Allowed Multiplier 244
- Relay Denied Multiplier 244
- Relay Server 198, 200
- Remember recipients for Webmail 241
- Remote Access 79
- Remote users 74, 167
- Remove VPOP3 service 456
- Rename folders 130
- Replicating VPOP3 314, 323
- Report
 - Largest Folders 425
 - Messages Received 422
 - Messages Sent 423
 - Messages Summary 424
 - Quotas 426
 - SMTP Server Status 428
 - SMTP Usage 429
 - Spam filter 431
- Report bad mailer_daemon messages to administrator 383
- Requirements 11
- Restore backup 91
- Restore Messages 320
- Restrict receiving from particular address 115, 226
- Restrict sending to particular address 115, 226
- Restricting access to VPOP3 services 269
- Return Address 159, 165, 207

- Return Path 207, 373
 - Return path for autoresponses 302
 - RFC 3834 302
 - RFC 5451 372
 - Route by parsing message headers 188
 - Route mail 167
 - Router 173
 - Routing 100
 - Routing options 188
 - Rule Weights 452
- S -**
- Satellite 170
 - Script
 - IDS Logging 445
 - Signature 445
 - Scripts 444
 - Search subject line for a marker 188
 - Searching in grids 92
 - Security Settings 392
 - SECURITY.LOG file 325, 469
 - Send Admin message 144
 - Send all messages to a specified user/list 188
 - Send all quarantine reports to 397
 - Send database backup successful email messages to administrator 305
 - Send Quota 426
 - Send welcome message when moderator adds list member 158
 - Sender Blacklist 115, 379
 - Sender Prohibited error message 226
 - Sender Whitelist 115, 379
 - Sending different messages through different Senders 210
 - Sending Mail through different servers 204
 - Sending Messages 197
 - Sending messages to VPOP3 users as administrator 144
 - Sent Message Report 423
 - Server access blocked temporarily 394
 - Server access not allowed 249
 - Server access temporarily blocked 394
 - Server access temporarily blocked! Please try again later 244
 - Server to send ETRN to 195
 - Service bindings 273
 - Service Controller 456
 - Session Encryption 180, 200, 216, 220, 223, 248, 261
 - Signature 339
 - Customising 445
 - Signatures
 - For internal messages 124
 - For outgoing messages 123
 - Simple Mail Transfer Protocol 60, 62
 - Size dependent forwarding 100
 - Slow Message Posting 159, 165
 - Smarthost 198, 200
 - SMTP 60, 62, 451
 - ATRN 64
 - Authentication 62
 - Banner 241
 - ETRN 64
 - Host Name 241
 - SMTP Authentication 200
 - SMTP Client Processor 347
 - SMTP Direct 198, 203
 - SMTP Direct Sending 204, 451
 - SMTP Feed 195
 - SMTP Filtering 225
 - SMTP Incoming 176
 - SMTP MX Sending 204
 - SMTP Options 195
 - SMTP Port 200
 - SMTP Relay 198, 200
 - SMTP Relay Servers 200
 - SMTP Return Path 207
 - SMTP Rules 225, 226, 447
 - SMTP Server 241
 - SMTP server should collect email addresses for authenticated users 241
 - SMTP Server Status Report 428
 - SMTP Usage Report 429
 - Socks Proxy 382
 - SOCKS proxy server 175
 - SOCKS server address 382
 - SOCKS server port 382
 - SOCKS server user name 382
 - SOCKS V4 Proxy Settings 382
 - Sort quarantine reports by 397
 - Spam
 - Don't archive 361
 - Spam bounce messages 373
 - Spam Detected Multiplier 244
 - Spam filter 125, 395

Spam filter 125, 395
 Bayesian Database 399
 DNS resolution 406
 File loading problems 406
 Files 406
 Report 431
 Rule weights 404
 Rules 404, 452
 Script 452
 SMTP 225
 Timeout 406
 Weights 452

Spam Quarantine Threshold 125
 Spam Redirection 159, 165, 401
 Spam subject prefix 401
 Spam threshold 159, 165, 401
 Spamfilter Quarantine 397
 Speed up processing of pending messages to main store 361
 SSD Drives 325
 SSL 59, 60, 66, 200
 Standard Subject Prefix for autoresponses 302
 STARTTLS 66, 200
 Status Monitor 58, 458
 stls 66
 Store and Fwd email target 125
 Store and Fwd target server 125
 Submit button 92
 Subnet Mask 436
 summary.log file format 455
 Support IMAP IDLE command 249
 Syntax Error Multiplier 244

- T -

Target Backup Size 369
 Target Blacklist 115, 379
 Target File Network Password 305
 Target File Network Username 305
 Target Whitelist 115, 379
 TCP/IP ports 273
 Temporarily blocked 394
 Temporarily reject incoming SMTP on Spam filter timeout 406
 Temporary Filename 305
 This list is a digest of ... 159, 165
 This list is confidential 158
 This server requires SMTP authentication 200

Throttling bandwidth 274, 388
 TLS 59, 60, 66, 200
 Too many concurrent searches - try again later Error Message 249
 Too many connections from this address! Error Message 249
 Too many current FETCHes active Error message 249
 Too many logins for this user Error Message 249
 Toolbar 92
 Trace messages 333
 Troubleshooting login problems 469

- U -

Undelete Messages 125, 311
 Uninstall VPOP3 service 456
 UpdateBayes 454
 Use a custom unsubscribe message 158
 Use a custom welcome message 158
 Use Assistants between 100
 Use dynamic Spam Filter thread priority boosting 406
 Use ETRN 195
 Use Fastest POP3 Download method 383
 Use Forwarding 100
 Use Forwards between 100
 Use From: header address in SMTP envelope 383
 use HTTP Proxy 382
 Use ODBC database as well as local database 255
 Use this Mail Collector with these Connections 179
 User 125
 Aliases 118
 Assistant 100
 Comments 97
 Email Addresses 118
 Forward 100
 Groups 97
 Mappings 118
 Passwords 98
 User can set forwards to these addresses 103
 User VPOP3 directory as working directory 369
 User welcome message 143
 userlist.csv 140
 Username to access Main Store 361
 Users
 Adding 94, 141
 Bulk Editing 145

Users

- Deleting 131
- Editing 76, 92, 96, 145
- Export to file 140
- Grey 97
- Greyed 94
- Import from File 136
- Import from Windows users 139

- V -

VDSL 170

Verbose Output 140

Verify list subscriptions 158

Verify Network Login Details 305

View event log 244, 392, 394

Virus scanner 11

VPN Server 81

VPOP3

- Service Controller 456

VPOP3 Basic 59

VPOP3 Daily usage Summary 358

VPOP3 Enterprise 59

VPOP3 Home User 59

VPOP3 IP Address 85

VPOP3 Server access temporarily blocked 394

VPOP3 Service 58

VPOP3 Status Monitor 58, 458

VPOP3.EXE 58

VPOP3DB Service 58

vpop3postgres user 450

VPOP3-SPAM 401

VPOP3STATUS.EXE 58, 458

vpop3svc.exe 58, 456

- W -

Wait for up to X seconds for an incoming SMTP connection 195

Webmail 60

- Email addresses 103
- Real name 103

Welcome message 143

When to backup database 305

Whitelist 401, 452

Whitelist Local Addresses 401

Windows passwords 392

Windows Username 125

- X -

xDSL 170

X-VPOP3-ORIGRCPT 241

X-VPOP3-Spam 452

- Y -

Your connection has been blocked temporarily - try again later 244

- Z -

Zip archived messages 369