MarshallSoft Client Mailer

Email Servers

Version 6.0

May 10, 2021

This software is provided as-is.
There are no warranties, expressed or implied.

MarshallSoft Computing, Inc.
Post Office Box 4543
Huntsville AL 35815

Email: info@marshallsoft.com
Web: www.marshallsoft.com

TABLE OF CONTENTS

1 Introduction

The **MarshallSoft Client Mailer (MCM)** is designed for software developers and database programmers. **MCM** is a software component that provides the capability to send **personalized** email to your clients or customers **directly** from your application program, programmable database or spreadsheet! Product information for the **MarshallSoft Client Mailer (MCM)** can be found at http://www.marshallsoft.com/mcm.htm.

This manual contains background information on SMTP, POP3, and IMAP servers.

An email account is required in order to use the **MarshallSoft Client Mailer**. An account used <u>only</u> for sending email with the **MarshallSoft Client Mailer** is strongly recommended, although an existing account can also be used.

There are several categories of email servers in common use, as outlined in the following sections. If you already have an email account and are not sure of what type of email servers it supports, first read through the following sections to become familiar with the various types of servers, then look through the account information of your regular email client (Outlook, etc…). In particular, look for the information as follows.

For <u>SMTP</u> (outgoing email):

1. The SMTP server name.
2. SMTP port (25 or 587) used.
3. If "SMTP Authentication" is supported, the SMTP username and password will be needed.
4. Whether or not TLS/SSL is required.

Note that the user name and password for SMTP is often the same as for POP3.

For <u>POP3</u> (incoming email):

1. The POP3 server name.
2. The POP3 port is always 110.
3. The POP3 username and password.

2 Choosing an ISP

If you already have a suitable ISP (Internet Service Provider), it is best to create an additional email account for sending email to your customers. Virtually all ISP's allow multiple email accounts without any additional charge.

2.1 ISP Limitations

When choosing an ISP, look for one that:

1. Supports "Authenticated SMTP" (see Sections 3.3 and 3.4 below).
2. Does <u>not</u> require TLS/SSL.
3. Does <u>not</u> impose "unreasonable" limits on the number of emails that can be sent.

ISP's often impose one or more of the following kinds of limits on sending email:

1. Limits on the number of emails that can be sent during one connection.

This is by far the most common limitation. The solution is to close and reopen the connection just before the email send limit is reached. This can be done automatically by MCM using the "ReOpen" parameter when calling the mcmSmtpConnect function.

2. Limits on the number of emails that can be sent, counting all connections from a single IP address.

This limitation is not very common, but it does effectively prevent the use of multiple connections, which are necessary to be able to reduce the time necessary for sending email to large numbers of recipients. Avoid using an ISP with this kind of limitation.

3. Limits on the number of emails that can be sent within some time period.

The time period may vary from as little as 5 or 10 minutes to up to a month. It is best to avoid ISPs that impose severe limitations of this type. Read the text file Smtp2Go.txt

4. Limits the number of connections that can be made from any one IP address.

This limitation is not very common, but prevents using multiple connections. Avoid ISPs that impose this limitation.

2.2 Workaround for ISP Limitations

The best workaround or solution is to find an ISP that does not impose stringent limitations on the number of email messages that can be sent. Very few ISP's will allow unlimited sending, but some impose significantly more stringent limitations than others.

Another possible "workaround" or solution is to install an email server on your own computer. However, more and more ISP's are limiting connections to port 587, which prevents you from running your own server since that requires port 25. Further, many (if not most) email servers will reject your email since your server will not match the server record for your domain name.

2.3 Web Based Email Servers

Web based email servers such as Gmail, Hotmail, and Yahoo all impose quite strict limitations on the number of email messages that can be sent. They are also very slow and require the use of the TLS/SSL web protocols.

Also see the section "*Free Email Servers*" in the MCM User's Manual (mcm_users.pdf).

3 SMTP Servers

A connection to a SMTP server must be made to be able to send email. There are several common configurations for SMTP servers.

3.1 Standard SMTP on Port 25

Standard SMTP servers do <u>not</u> use usernames or passwords. If connecting to the Internet through an ISP (Internet Service Provider), then that ISP will normally provide a SMTP server. However, if you connect to that same ISP and you are not connected to the Internet through them (say you are travelling with your laptop), then you will not normally be able to send email since this is considered "relaying".

There are several workarounds for the "relaying" problem, such as "read before send", depending on your particular ISP.

3.2 Standard SMTP on Port 587

Most ISPs are moving from using port 25 to using port 587. Only "well known" servers are allowed to use port 25, which prevents connecting directly to the SMTP server associated with the email account of a recipient.

3.3 Authenticated SMTP on Port 25

SMTP Authentication employs a username and password to identify the user to the server. These two entities are often the same as the username and password of the corresponding POP3 (or IMAP4) account.

It is not necessary to be connected directly to your ISP in order to do SMTP Authentication. The "no relay" problem does not exist since the authentication identifies the client to the server.

3.4 Authenticated SMTP Port 587

This works the same as using SMTP Authentication on port 25, except that port 587 is used instead.

This is the most commonly used configuration.

3.5 TLS/SSL Authentication

Most web based email services (such as Gmail, Hotmail, Yahoo mail, etc.) require the use of the TLS/SSL protocols.

To use these servers, one must connect to them through a TLS/SSL proxy server (such as the free STUNNEL server). Refer to http://www.marshallsoft.com/stunnel.htm for more information.

Note that web-based SMTP servers have by far the most severe limits on the number of emails that can be sent. For example, Gmail, Yahoo, and Hotmail are popular web based email servers, but all impose quite severe limits on the number of emails that can be sent.

3.6 Free SMTP Servers

There are a few free SMTP servers that can be used to send out email. However, as you might expect, there are severe limits on the number of email that can be sent, and theses limits can be changed at any time for any reason without notice..

Also, some of these SMTP servers may be reading your email for marketing purposes. For insight into this situation , google "gmail email mining"

GMAIL (https://www.gmail.com) provides a SMTP server that can be used for free, but requires TLS/SSL encryption. Read section 7.0 below "GMAIL Security".

There are other free SMTP servers, such as SMTP2GO (https://www.smtp2go.com/), which supports SMTP Authentication but does not require TLS/SSL encryption.

However, although MCM can be used with free SMTP servers, we do not recommend their use.

4 POP3 Server

A connection to a POP3 or IMAP4 server must be made in order to read email. However, POP3 is by far the most common protocol for reading email from an email account.

The well-known port for POP3 servers is port 110. Both an account username and password are required.

5 IMAP4 Server

Unlike the POP3 server, an IMAP4 server allows the use of multiple account folders.

The well-known port for IMAP4 servers is port 143. Both an account username and password are required.

6 Your Customer's ISP

If you are building an email application that will be distributed to your customers, you have two choices in selecting the SMTP server that your application will use.

6.1: Use Customer's SMTP Server

You can code your application to use your customer's SMTP server. This is commonly done, but can sometimes be tricky because:

1. Your customer may have no idea what email parameters he is using, which may require your assistance.
2. Your customer may use only web based email, which means that he may never have set up an email account which uses a SMTP server.
3. Your customer may use several email accounts, each using a different SMTP server.

6.2: Use Your SMTP Server

One solution is to setup a SMTP server for use by all of your customers. For some email applications, this is the preferred solution as this does not require your customer to specify email parameters, minimizing support calls from them.

That said, it is not a good idea to use a national web-based free ISP such as Gmail because such free SMTP servers impose strict restrictions on the number of email that can be sent.

7 GMail Security

Gmail "Insecure Sign-in Technology"

Google is promoting a new security standard (OAuth 2.0), which prevents almost all non-google email clients from connecting to Gmail servers. You can continue to use the industry standard TLS/SSL by editing your Gmail security settings at https://www.google.com/settings/security/lesssecureapps

Gmail doesn't recognize periods as characters within usernames. Remove all periods from user names passed to SEE functions. See https://support.google.com/mail/answer/10313?hl=en

8 OAUTH Delegation

Some web based email services, such as Gmail and Yahoo, are requiring "OAUTH Delegation ".

See section 16 "OAUTH Delegation" in the MCM User's Manual mcm_users.doc, which is also online at http://www.marshallsoft.com/mcm_users.pdf