This article is intended to give you a general understanding how ArGoSoft Mail Server Pro, and en Email, in general, works. It does not give you step-by-step instructions; it does not walk you through menu commands, and does not describe all settings of server. To see descriptions of individual, advanced features of server, please use the help file, which is distributed with mail server. We will be constantly updating this document, according to questions we are receiving from our users.

Friday, June 21, 2002

Introduction

Thank you for choosing **ArGoSoft Mail Server Pro**. It is the most easy to use, and the most compact mail server on the market. It can perform most basic email tasks, and much more than that. Our server will provide you with reliable email service. It is fully functional server, which supports most popular protocols, SMTP, POP3, also Finger, and has built-in Web server, which will give users of your server an access to their email via any Web browser, which supports HTTP 1.0 or later. Web Interface also can be used to administer server.

SMTP stands for Simple Mail Transfer Protocol, and is used for **sending** Internet mail. Your email client (software, which is used for sending or retrieving mail, such as *Outlook*, *Outlook Express*, *Netscape*, *Eudora* and so on) uses this protocol to connect to your server, and transmit to it mail. Your server uses the same protocol (SMTP) to relay email, transmitted by your client, to the destination server. And, remote servers are using the same protocol to deliver mail, addressed to the users of your server.

POP3 stands for Post Office Protocol, version 3. It is the most wide spread protocol for retrieving mail. Your email clients are using this protocol to retrieve mail from your server. Another popular protocol for retrieving mail is **IMAP**. *ArGoSoft Mail Server Pro*, currently, does not support it.

Finger protocol is used for retrieving information about users of your server. It was very popular during the early years of the Internet. Currently, very few networks are using it.

How Does Email Work

We included this section in order to help our users better understand how our server, and Internet mail, in general, works.

First, you have to tell your server, which domains are local. Local domains are those, which are served by your server. If the domain is local for your server, and server receives an email, which was sent to the domain in the list of local domains, it will not attempt to relay mail to the Internet, it will treat the mail as local, and store it to the local user's mailbox. You are defining local domains from *Tools - Options – Configuration* dialog box.

Now, let's assume, that you want to send an email to the address *joe@somewhere.com*. You are composing an email in your favorite email client, and clicking *Send* button. The client will connect to your server, using SMTP protocol, and relay your message to it.

After your server receives the mail, it looks at the address of recipient, picks up the domain *somewhere.com*, and looks whether it is local.

If the domain **is local**, then server treats the address as local, and stores the message locally, in the mailbox, which belongs to user Joe, at the domain *somewhere.com*. Message just sits in Joe's mailbox, and waits until the owner of mailbox, Joe, retrieves it, using his email client, via POP3 protocol. The voyage of the message ends here.

If the server finds, that the domain is **not local**, it is *not* listed in the list of local domains, it attempts to determine an address of server, which is responsible for that particular remote domain, and for which server the domain *is* local.

This server is called **Mail Exchanger**, and, information about it is stored at DNS server (you have to provide address of DNS server, when setting up your server). A domain can have one or more exchangers. Domain may not have an exchanger at all. And, one exchanger may serve multiple domains. All depends on the size of the organization, which uses the domain, and capacity of mail server software, which is used as exchanger.

And, as you probably guessed, your Server is an exchanger for your local domains.

So, let's return back to the point, when your Server retrieved the list of Mail Exchangers for destination domains. This list is also known as a list of **MX records**. As we mentioned, domain may not have MX records. In this case, your Server will assume that domain name *itself* is an address of server, which serves the domain.

After getting this information from DNS server, your server attempts to connect to *Mail Exchangers*. At this point, your server acts as email client, and in case of successful

contact, transfers your mail using SMTP protocol, exactly the same way as your email client did, when it transmitted your original message to your server. And, after receiving mail, remote server does the same work, as your server did: checks the domain of recipient, and finds that it is for it's local user (it has to be local, since the server is an exchanger), and stores mail to the local mailbox, which belongs to Joe.

After that, when Joe decides to retrieve the mail, he runs his email client, similar one which you used to send mail, and retrieves your message using POP3 protocol. Here, the trip of your message ends.

Installation

To install the Server, double-click the file *mspro.exe*, which can be downloaded from

http://www.argosoft.com/mailserver/

And follow easy step-by-step instructions.

If you are having problems, then follow steps, described in Troubleshooting section (Manually installing and uninstalling mail server).

Configuring Your Domain

Server can be used on any network with TCP/IP support. It can be the Internet, Intranet, or even single computer, with TCP/IP installed on it.

Probably, the most useful use of the server will be its use for Internet mail.

Probably, you already have one or more domain names. If you don't, you still can receive email, since you can use IP address of your server computer as domain name. But, if you use IP address, you should be aware, that you might encounter problems with certain networks, which do not support IP addresses as domain names. Besides, domain names are much easier to remember, then IP addresses, and probably, you want to give your users easy-to-remember email addresses.

So, you already have domain name(s), and want to set up your email server, so that it serves your domains, acts as *Mail Exchanger* for them.

First, you have to make sure, that your domains are set up properly with DNS system. If your domain does not have MX record, then it should point to your Server computer. If it does have one, or more than one, then the one with the highest priority should point to your Server computer. For understanding MX records, see the chapter *How Email Works*.

Most likely, you will have to contact your ISP, and ask them to add proper MX records to your domain. Just tell them, that you want to host your mail yourself, using your own server, and ask them to make appropriate changes with DNS server.

Your Server has built-in utility, which allows you to find out whether you are ready to host your domain(s). You can access it by clicking *Tools – Domain Information* menu item.

Just run the utility (don't forget to specify DNS server in *Tools - Options – General* box), and, in *Domain Name* box, type the domain name you want to test. Then, drag away *Domain Information* dialog, so that you can see your mail server log underneath it, and click *Go* button. Utility will attempt to resolve MX records for the domain, and connect to exchangers. If you see that you are connecting back to your server, if there is an activity in the log, which says that there was an attempt of SMTP connection, it means that you are ready to host that domain.

ActiveX version of the same utility can be accessed at:

http://www.argosoft.com/applications/mailserver/domaininfo.asp

Configuring Your Server for Internet Mail

First, you will have to tell your server which domains are local.

You will have to decide, whether you want to add your local domains as aliases to the blank domain, or as a top-level domain.

If you have only one domain, we would recommend adding it as an alias of blank domain. It will allow you to access user mailboxes by using only user name, without appending the domain name to the user name. Disadvantage of this method is, that, if you have more than one domain, and you want to have two or more accounts with the same names, you will be unable to do that, if your domains are aliased to each other.

So, let's assume, you have only one domain, *mydomain.com*. Click *No domain* entry in configuration box, select properties, and in *aliases* box type *mydomain.com*. Click OK.

Click *New* button on the toolbar, and fill in *User properties box*: Enter user name *Joe*, password and confirm password (type whatever you want, main thing is – content of both boxes must match), then click OK. User *Joe* will appear in the right side of configuration box. Now, if Server receives mail addressed to *Joe*, without the domain, or *joe@mydomain.com*, it will place it in Joe's mailbox. Note, that both, blank domain and name at domain addresses point to the same mailbox.

If you have another domain *domain1.com*, you can add it to the aliases of blank domain, and the address *joe@domain1.com* will also point to the same mailbox *Joe*. It means, if

you want to have two separate mailboxes *joe@mydomain.com* and *joe@domain1.com*, there is no way to do that, if two domains are aliased.

To use domains, which are not aliased, you have to create another top-level domain. Click small down arrow next to "*New*" button, select *New Domain*, and type your domain name, e.g. *domain2.com*. Now, you can create an account *Joe*, which is associated with *domain2.com*. Just highlight *domain2.com* in a right pane, and add user *Joe*. After you have done that, you will have two mailboxes, named *Joe*. The addresses Joe, *joe@mydomain.com*, *joe@domain1.com* will point to one mailbox, while *joe@domain2.com* - to another.

Now, you have to specify essential settings in Options dialog box, which can be accessed via Tools – Options. If you intend to send mail to the Internet email addresses (most likely, you do), then you must enable relay, by checking Allow Relay box. You also must specify an IP address of DNS server, which will be used by your server to retrieve MX records of destination domains.

So, since you already have configured MX records for your domain, and added users to your server, you should be able to use your server. Mail sent to your domain should be arriving to your server, and you should be able to retrieve mail from it, and send mail using it.

To retrieve and send the mail, you will have to set up your email clients. Since you already added MX record, it means, you already know the domain name of your computer, and, you just can use it as SMTP and POP3 server addresses in your email client.

Protecting Your Server from Unauthorized Use

If you don't enable one of the security features of Server, it can be used by anyone on the Internet to relay mail, and you will become so called Open Relay. You may even get listed at Open Relay Database (ORDB, see next section), and other servers will refuse to accept mail from you, because you will be a potential source of junk mail.

Pro version of Server contains several features for protecting your server from unauthorized use. Please note, that these features do not apply to the mail delivery to your local recipients. If you want to protect your users from unsolicited mail, see section "Protecting Your Users from Spam".

SMTP Authentication – in our opinion, is the most reliable method of protecting your server. If it is enabled, server will require user name and password from users in order to relay mail to the Internet. It can be enabled from *Tools – Security – SMTP Authentication* box. Drawback of this method is that your clients will have to enable SMTP Authentication in their email clients, and it requires additional steps from them. Besides, not all email clients, especially, older versions, support it, because this method is relatively new.

Another feature is **Trusted IP addresses**. You can list IP addresses of computers from which your server will always accept mail for relay, no matter whether they have authenticated or not. Of course, this option makes sense only if you have enabled SMTP authentication, if you did not, then all IP addresses will be trusted IP addresses. This option is good if you know that your users will be connecting to your server only from fixed IP addresses, and, it is not always the case. Trusted IP addresses can be set up from *Tools – Security – Trusted IP Addresses* box.

And, the last feature for protecting your server is **Sender Rules**. If this option is enabled, server will not accept mail for relay if either domain name, or an account of sender (which was received with RCPT TO SMTP command), does not belong to your local addresses. This method should work for most cases, but it is not reliable, because anyone can use any return email address in email client, and "cheat" your server very easily.

Protecting Your Server From Spam

You also may want to protect your users from unwanted mail. Following features apply only to the local delivery of mail to your computer.

Pro version of the Server interfaces with services provided by two organizations: **ORDB** (Open Relay Database, http://www.ordb.org), and **MAPS** (Mail Abuse Prevention System, http://www.mail-abuse.org).

The ways ORDB and MAPS work are similar. Both organizations maintain the databases of known potential sources of junk mail. MAPS has multiple databases, while ORDB has only Open Relays database. But, ORDB is more reliable, since they are listing IP addresses of servers individually, while MAPS may list entire batches of dial-up accounts of entire ISPs, and, there is more danger that your users will lose important mailings.

MAPS and ORDB can be enabled from *Tools – Security – MAPS/ORDB*. If MAPS and/or ORDB options are enabled, server will not accept mail for local delivery if IP address of connecting computer is listed with databases. You should know, that Server uses direct DNS queries with ORDB and MAPS databases, and will require more resources from your Server.

You also can use **Filters** and **Attachment Filters** for protecting your users.

Filters feature (*Tools – Security – Filters*) allows you to filter any message, which goes through your server. You can specify sequences of characters, and if they are found either in message headers, or message body (depending on your selection), then server will not accept mail.

Attachment Filters (*Tools* – *Security* – *Attachment Filters*) act the similar way, but they are looking for certain type of mail attachments to email messages.

Note, that both Filters and Attachment Filters will be scanning any message, no matter whether they are sent to local, or remote recipients.

Beginning from version 1.8.1.4, Pro version of server also supports individual filters and attachment filters. They work the same way as filters and attachment filters, described above, but they will apply to the individual user. To set up them for specific user, click Tools – Configuration, select an user, then click Properties button on a toolbar, and go to Filters tab.

Note, that filters and attachment filters will not work, if you are allowing unlimited message size on the server (Tools – Options, Advanced tab, Maximum Message Size box).