



Using WinGate 6 Email

Concepts, Features, and Configurations.

Neil Gooden
Qbik New Zealand Limited
Rev 1.0 December 2004

Using WinGate 6 Email: Concepts, features and configurations	2
Introduction.....	3
Basic Email Concepts.....	3
Differences in mail between WinGate 5 and WinGate 6.....	4
WinGate Mail Features:.....	6
Domains & Email Handlers.....	6
POP Collection.....	8
Secure Bindings.....	9
Controlling Mailboxes.....	9
Anti-Spam Measures.....	10
Mail Server Scenarios and Configurations.....	11
Scenario 1:.....	11
Scenario 2:.....	25
Scenario 3:.....	43
Scenario 4:.....	64
Scenario 5.....	75

INTRODUCTION

This document explains WinGate's mail server features, including an in-depth discussion of several common scenarios in which it can be used and the benefits its use can bring.

This is intended to complement the WinGate help file, giving new users simple to follow set-up guides, and for advanced users, greater detail regarding specific features.

Basic Email Concepts

Before discussing specific mail features of WinGate, it is important to understand some basic concepts of email in general.

In a nutshell, email systems have the task of transferring email messages from a sender to a recipient (or several). This transfer may take place in several different ways. If we look at the typical life of an email message, the different types of exchange can be highlighted. This can provide good insight into how WinGate mail works, and can be used, and also where to look for any problems that may arise.

The first step is composition, a person or sometimes an automatic program creates the email content. Obviously there is no point to an email unless there is an intended recipient. So, you have an email, and you know where you want it to go, what next?

This is where the concept of **delivery** comes in. Your email software will be configured with the address of a server to which it is to submit all email you write for delivery. When you hit the send button on your email client, it makes a connection to this server, and talks a special language to the server to tell it what to do (the particular language used is called a **protocol**). In this exchange of information, the email client tells the server who it is, who the message is from, who to deliver the message to, and gives the body of the message to the server. The server indicates to the client whether it will take responsibility to deliver the message or not.

Typically with internet and frequently with internal company email, the protocol used for delivery is called the Simple Mail Transfer Protocol (SMTP). There are also other methods, such as file copying, X.500 etc. The first stage of delivery (from the client to the first server) is nearly always done using SMTP, and this is the method supported by WinGate mail. If you are interested in further information on this protocol, check out the full specification at <http://rfc.net/rfc2821.html>.

The mail server then checks to see whether the email is destined for a local mailbox (typically a file folder on the server where email for a particular user is stored), or needs to be **relayed** – i.e. passed on to another server for delivery. If the destination is a local mailbox, typically the file will be moved into the mailbox folder, and that is the end of the delivery phase. For external mail however, there will be at least one more server involved. Your server will typically look up which servers are advertised as accepting mail for the **domain** specified in the recipient's email address (the part of the address after the '@' symbol), and then connect as a client to each of these servers to attempt to deliver the mail. This transaction also typically uses SMTP.

Eventually the email will either be successfully copied into a mailbox somewhere, or if there is a failure, then a Delivery Status Notification (DSN) will be generated by whichever server encounters the fault, warning the original sender that their

message was unable to be delivered. This is why it is important to specify the return address – who the email is from when it is delivered. The method that the server uses to look up which servers will accept mail for a domain, is based on DNS, a special type of DNS lookup known as an **MX lookup** (MX stands for Mail eXchange).

So, now there is an email sitting in a folder on a server somewhere. How does the recipient read it?

This is where the concept of *retrieval* comes in. The person who 'owns' the mailbox checks their mail, and it appears in their inbox. The process behind the scenes in this transaction involves the email client software making another connection and having a conversation with the server that looks after the mailboxes. This conversation uses a different language than SMTP – the most common one is called POP3 (Post-Office Protocol v3), but a common alternative is IMAP4 (Internet Mail Access Protocol v4). These are mailbox access protocols, rather than mail delivery protocols.

On the internet, each well-known protocol (which POP3 and SMTP are) has a standard port that it operates on, for SMTP this is port 25, and for POP3 it is port 110. (For more information about ports see <http://www.iana.org/assignments/port-numbers>). These are the ports that WinGate's SMTP and POP3 servers listen on for connections.

Differences in mail between WinGate 5 and WinGate 6.

For those of you familiar with WinGate 5, there have been significant changes in email in WinGate 6. WinGate 5 Mail was fairly simple, and performed the basic aspects of a mail server, but could sometimes become rather limited in its configurability. With WinGate 6, Qbik has taken this basic mail server, and extended it in many different ways, improving virtually all areas of operation, as well as adding numerous new features. These are explained more fully in the next chapter, however, here are some of the highlights of WinGate 6 Mail:

- The ability to have per-user per-domain configuration control.
- SMTP and POP3 Service bindings now allow you to accept SSL connections. This means that secure mail can be set up using SSL, and provides Outlook mail users with a highly secure mail option. A different certificate for SSL can even be used per network interface,
- The Mail Queue window has been added to GateKeeper. This shows details of all the queued domain jobs, and messages that are queued remotely, and provides the ability to abort jobs, delete messages or force queue processing.
- Enhanced support for TLS connections (to send mail over an encrypted connection) and for SMTP authentication to remote mail servers. This can be configured on a server by server basis, so that trusted email networks can be set up between servers that support NTLM, CRAM-MD5 or SASL PLAIN Authentication.
- Several new additions to WinGate's SMTP receiver, specifically designed to combat spam. These include:

- IP vs. email domain verification, based on MX and PTR->A record lookups.
 - optional blocking of numeric sender domains for untrusted senders
 - optional blocking of blank return-path for untrusted senders.
 - attachment blocking.
-
- POP3 collection has been added. Email can now be retrieved by WinGate from any number of POP3 accounts and delivered to different locations (local or remote), depending on configuration. This allows users to integrate multiple mailboxes, or allows you to share a mailbox at your ISP.

WINGATE MAIL FEATURES:

Domains & Email Handlers.

WinGate 6 introduces new ways in which domains and their associated addresses can be handled, thus allowing for greater configuration flexibility. As these two concepts, Domains and Addresses, are closely linked this description of Domain handling will cover both areas.

When a Domain is entered in WinGate, it can be configured in several different ways. The possible options are shown under Default delivery method, in the Edit email domain dialog.

If WinGate is to act as the primary mail server for the domain then the top option 'Mailboxes for this domain are hosted on this server' would be selected as WinGate will be the end point for the domain's email. Thus by default, when WinGate receives an email it will process it and try to deliver the email to a local users account.

However, if WinGate is not to be the end point for the domain's email then the second option would normally be selected 'Mailboxes for this domain are hosted on another server'. This can mean that another machine on the internal LAN is the primary mail server for the domain, or it could be that another machine on the internet is the responsible mail server for the domain. This information is entered in WinGate via the Remote delivery options, which can be accessed via the '...' button once this delivery method has been chosen.

There are two ways WinGate can be configured to deliver to domains that have been specified as remote. By default, it will try to use DNS (an MX record lookup) to discover where the remote server is, that is responsible for the specified domain. However, a custom setting can be entered to override this behaviour and point to either another domain name, or an IP address, that could be located either internally on the LAN or externally on the internet.

Irrespective of whether WinGate is locally hosting the domain or the mailboxes are hosted by another server, an additional setting can be made to 'Redirect all mail' to a specified user / mailbox. If the domain is being hosted locally by WinGate, then this option provides a drop down list of all users in the WinGate user database that have been enabled for mail. If, on the other hand, mailboxes are being hosted on another server, then this option allows for the free text entry of a full email address for the mail to be redirected to. This redirect acts as an 'instead of' option rather than a 'copy to'; i.e. if all mail is to be redirected to Neil, and an email is received for Bob, and Bob has no email handler override, then this email will be sent only to Neil and not to Bob, even though he was the specified original recipient.

Which brings us on nicely to the User / Addresses configuration, and the use of Email Handlers.

Email handlers need to be added to the domain, as it is these two pieces of information (the email handler and the domain) that create the email address. An email handler could be a user name that already exists in WinGate or an 'alias' that points to a user within WinGate. There are several ways WinGate mail can deal with these email handlers.

By default the screen will appear blank, with the option 'Enable reception of mail for addresses where no matching address handler exists' ticked. This setting will have a slightly differing effect depending on which Default delivery method had previously been selected.

If the domain (and thus mailboxes) are being hosted locally with WinGate acting as the primary mail server, then when WinGate receives an email, it will see that there are no email handlers listed, and so will check the user database (be it NT or the WinGate DB) and if a match is found with a user that is enabled for email then the mail will be accepted and delivered, otherwise it will be rejected. So for example, if the user bob has been created as a user in WinGate, and an email is received for bob@yourdomain.com (presuming that yourdomain.com is the domain that is being locally hosted), then WinGate will see there is no message handler for bob, but as this option is ticked it will check the user database to see if bob exists there, and as he does, WinGate will accept the email.

But, if another server is hosting the mailboxes for the domain, then this option to 'Enable reception of mail for addresses....', when ticked, will have the effect of forwarding on all mail received to the remote server. If this option is unticked, then only emails that are addressed to users that have a specific Email handler will be forwarded to the remote server.

However, where WinGate mail really comes into it's own, and shows it's power and flexibility, is when individual email handlers are created for each user, giving 'per user - per domain' configurability for complete control over user's email accounts.

Email handlers should be viewed as overrides to the 'Default delivery method' changing or enhancing how WinGate processes mail for each particular email address. Thus the options available are the same, regardless of which Default delivery method has been selected.

When adding the email handler, the part of the email address before the @ needs to be entered as the address handler, and then the new delivery configuration can be added by ticking 'Override domain delivery settings'. The override delivery options available allow delivery to either a specific local mailbox / user, or delivery to a remote user / server.

The simplest reason for using email handlers when hosting a domain locally (with WinGate acting as the primary mail server) would be that only certain email addresses for a domain should be accepted. In which case the 'Enable reception of mail for addresses...' would be unticked. In this example, if the address handler was for 'bob', then the override setting would be to 'Deliver mail to local mailbox', with the destination of 'bob' selected from the drop down list.

A compelling reason for adding a specific email handler would be to redirect mail to a location that differs to where the domain's 'Default delivery method' would otherwise deliver it to, acting in a similar way to a forwarding tool. Thus, again using the example of WinGate acting as the primary mail server hosting the domain locally, if bob has left the company but would like email sent to his old work address forwarded on to him then the new override for the domain delivery options would be set to 'Deliver mail to another mail server' with the destination being set to the new email address that bob is now using, say bob@hotmail.com. And by leaving the Remote Delivery Option (accessible through the '...' button) as the default 'Deliver to any server responsible for the recipients domain (MX host)', all mail sent to bob will not be processed for local delivery, but instead queued up for remote delivery to hotmail.

An example of the power and flexibility of email handlers is the way in which they can be used as specific catchall channelers. I.e. in a similar case to above, where the domain (yourdomain.com) is being hosted locally by WinGate, and email is being received for neil@yourdomain.com, niel@yourdomain.com, and neal@yourdomain.com, but in fact this is just one user called Neil, who gets his email address misspelt regularly. Then 3 email handlers can be created so that if an email addressed to niel is received the handler's 'Override domain delivery setting' is to 'deliver mail to local mailbox' with the destination point to the user Neil, in the drop down list.

POP Collection

Another new concept in WinGate 6 mail is POP Collection. If mail for the domain is hosted on a remote server, such as with an ISP, then WinGate can now be configured (via POP Collection) to connect to this remote server, download the mail it is holding and then redistribute it to a user defined location. There are many benefits to this which include, more control over what is sent and received for the domain, AV scanning if the necessary plugin is installed within WinGate, plus, if the remote server is hosting the domain's mail in a catchall account, i.e. emails sent to jim@yourdomain.com and another sent to bob@yourdomain.com are both stored in the same mailbox on the ISP's server, then POP Collection can connect to this single remote mailbox, but separate out the mail in to all the different locally hosted mailboxes.

The set-up of POP Collection is fairly straight forward, with the Account details screen just needing to be configured with the remote server name or IP, and the username and password that the remote mailbox requires to allow access. Additional configuration to specify what type of secure connection needs to be made, if any, and whether or not to delete the messages from the remote server once they have been collected can also be set on the Account screen of the mail collection properties.

Once the mail has been downloaded, the second stage of configuring POP Collection is to specify how this downloaded mail should be processed for delivery. The default configuration for a new POP Collection is to parse the newly downloaded message headers and to deliver to any To: or CC: addresses it recognises. POP Collection can also be set to only deliver if the address parsed from the downloaded email matches a local mailbox, or to deliver all mail with un-recognised addresses to a default / catchall address.

It is at this point that other areas of WinGate mail come in to play. To parse these messages for acceptable email addresses, WinGate needs to have had two pieces of information pre configured elsewhere in the mail set-up; the domain name, and the users / email handlers. For information on Domains and Email handlers, how they are set-up and used in WinGate mail see the section above.

In the case of POP Collection, there are two different ways of setting up a domain, that this downloaded mail will be delivered to.

The simplest case, is to create a locally hosted domain, as described above, with the default reception option ticked for email handlers. This way, any mail that WinGate receives (either from an email client on the LAN, or by downloading from the ISP with POP Collection) will be processed and delivered into local mailboxes.

A different configuration that has the same end result, is to create the domain as 'hosted on another server'. The default reception for Addresses / email handlers should be unticked, as leaving it ticked will result in all downloaded mail being forwarded to the remote server, which, depending on configuration, could result in a mail loop. Thus specific override handlers for each user that is to have a local mailbox need to

be created, and the delivery set to override the domain default and deliver to a local mailbox selected from the drop down list. In this situation, if the POP Collection pulled down an email that was parsed and found to contain an address that did not have a handler, then WinGate would either not deliver it (ignore it) or would send it on to a default address

Secure Bindings

A new feature in the Enterprise edition of WinGate is the concept of 'secure' bindings utilising SSL and TLS, allowing for a connection between another computer and WinGate to be made across a secured channel. This other computer could be another mail server on the internet, or an email client on the internal LAN. The choice of whether to use SSL or TLS would depend on the scenario.

The choice of SSL, for example, would be useful if a corporate user on a LAN took a laptop home, and still wanted to send and receive mail securely. In this instance, a binding policy should be created in the POP3 server for the external interface, overriding the port number for the policy from 110 to 995 (as this is what most email clients use for secure POP, including Outlook and The Bat) and select to 'Use SSL' with a specific Certificate chosen from the drop down list. (For information about generating Certificates see the relevant section of the help file). SMTP would be configured in the same way, with a new bindings policy specified to 'Use SSL', except the port number for secure SMTP is 465 (although any port could theoretically be used).

However, the set-up would need to be different if a server on the internet wanted to send email to WinGate securely. It might be the case that a company has two offices (A and B), and wants internal email to be sent from office A to office B securely. In this scenario office B would create an SMTP bindings policy, specifying the external interface, overriding the port number from 25 to 465. At office A, a specific server should be entered to override the default delivery behaviour. This is done in the Mail server properties under the Servers option. Here the details of office B's server can be entered, including the customised port, and the choice to use TLS for the secure connection.

WinGate includes other secure mail features, such as various mail authentication methods. To learn more about WinGate mail security see the white paper on the WinGate website <http://www.wingate.com/resources.php?id=12>.

Controlling Mailboxes

Another addition to the WinGate 6 Mail server is the ability to have much greater control over user mailboxes. This is done through several different mechanisms.

Firstly there is pre-emptive control - the ability to control what is received (whether externally or internally) for a user, or more specifically, to control what is received for an email handler (see above for a description of what email handlers are and how

they work). Each email handler that is added to a domain, has the ability to apply extra restrictions over and above those globally defined in the Receiving pane. These extra restrictions include limiting the size of messages that the email handler can receive, blocking the handler from receiving attachments, as well as sending a copy of any emails sent to that handler on to another address, such as an administrator's or manager's.

Alternatively, there is control of a populated mailbox, limiting it's size through the use of quotas. Whereas the pre-emptive control revolves around email handlers, quotas revolve around user's in the user database, as a single user can have many email handlers (as explained in the email handlers section above). Access to the quotas is controlled through the user's properties, which is available from the Mailboxes pane in the Mail Server. By default no quota is set, but if selected, this will limit the size on the local disk to which a user's mailbox can grow. Once this limit has been reached, then mail for this user will start being rejected, until the size of the mailbox has been reduced or the limit raised.

Anti-Spam Measures

WinGate mail now also provides some built in anti-spam options. Although not intended as a stand alone spam blocker, it can help to dramatically decrease the amount of spam mail that is processed. Unlike other spam blockers, WinGate mail doesn't scan for words in emails, instead it tries to block spam from even entering the mail server for processing, terminating the connection at the 'Mail From:' email command. It does this by performing a number of checks on the server that is connecting to it, to send the (potentially spam) email. These options are found in the Receiving pane of the mail server properties, and an explanation of each can be found in the Help file.

The most powerful of these settings, is the option 'Block spoof sender address'. This allows the creation of either a 'black' or 'white' list of domains, which can then have checks performed against them. These checks involve a multi stage process, which includes reverse DNS lookups using MX records to verify that the domain sending to WinGate really is who they are purporting to be.

So for example, if a 'black list' were to be created, then the option 'Perform this check only for the cases listed below' should be selected. If it is desired that only sending servers that claim to be hotmail should be checked, then Add the rule that 'This criterion is met if - SMTP sender - contains - hotmail.com'.

Alternatively, if the checks were to be made on all mail servers that connected to WinGate mail, then the 'white list' option would be selected 'Perform this check for all cases except where list below'. The rules would be added just the same way as above, except this time the entered domains would be trusted by WinGate and not checked.

MAIL SERVER SCENARIOS AND CONFIGURATIONS

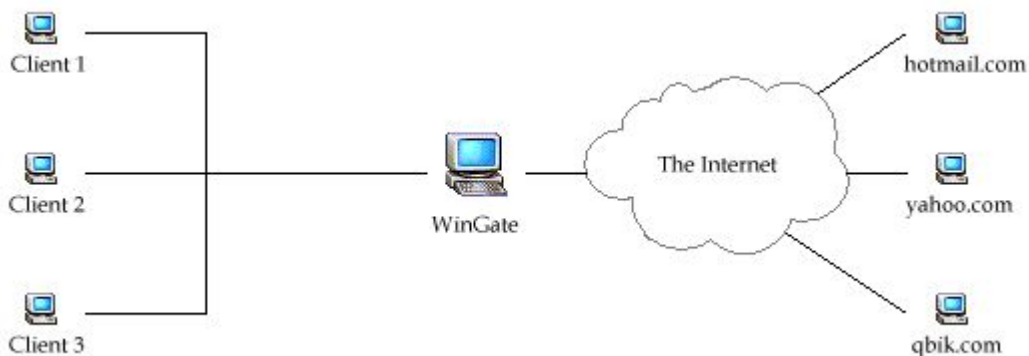
This section will detail a number of different ways WinGate mail server can be integrated in to common network scenarios.

Scenario 1:

Using Wingate as the main Mail Server on the network.

Computers on your
LAN
(Local Area Network)

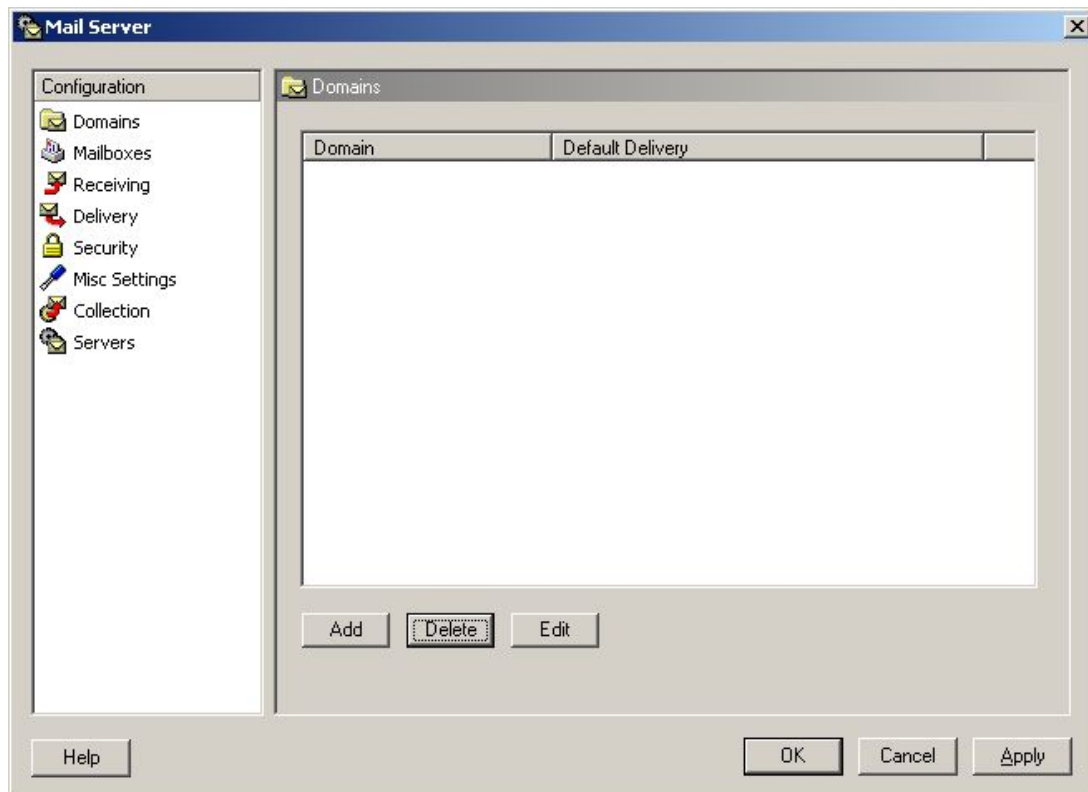
Internet Computers



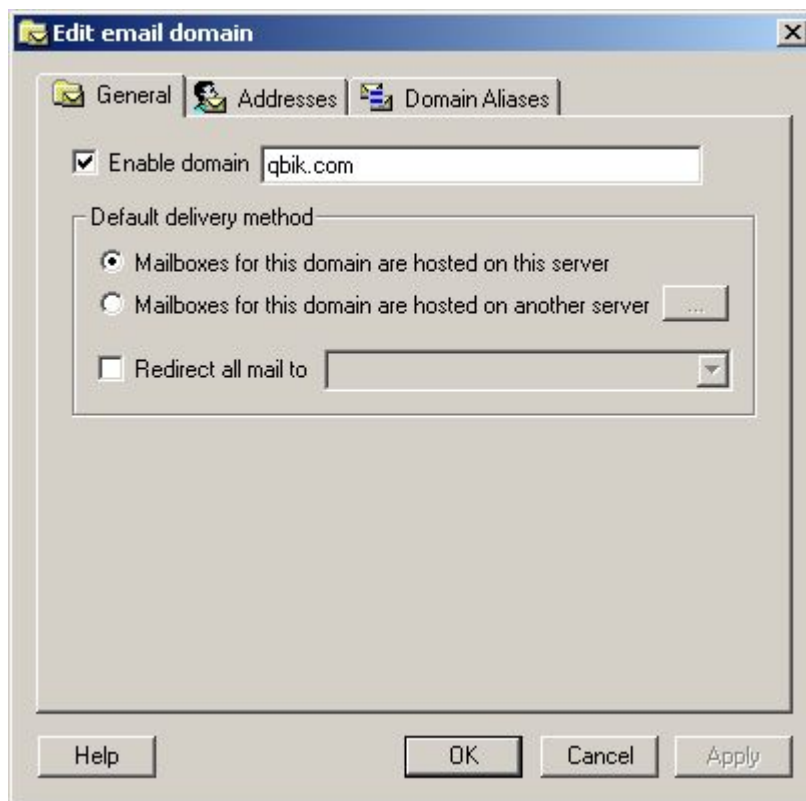
In the example above you would be using WinGate's built in mail server capabilities. Client computers (1,2, and 3) have their mail client programs (such as Outlook) configured to use the WinGate machine's IP address for SMTP and POP3. So, for example, if Bob is using Client 1 and wishes to send an email to Fred who has a hotmail address then, when Bob presses 'send' his mail program will connect to WinGate's SMTP server on port 25. WinGate then accepts the mail and begins to process it. As the message is destined for a hotmail address WinGate creates a connection to the Hotmail server and delivers the message. When Fred replies to this email the same path is taken but in reverse; so Hotmail connects to WinGate, which again accepts the message for processing. As Bob has an email address associated with his WinGate username, WinGate stores the email until Bob's mail client connects to WinGate (via POP3) and checks for any new mail.

If this is the configuration you are planning on using on your network, then you need to configure the Email settings in WinGate as follows.

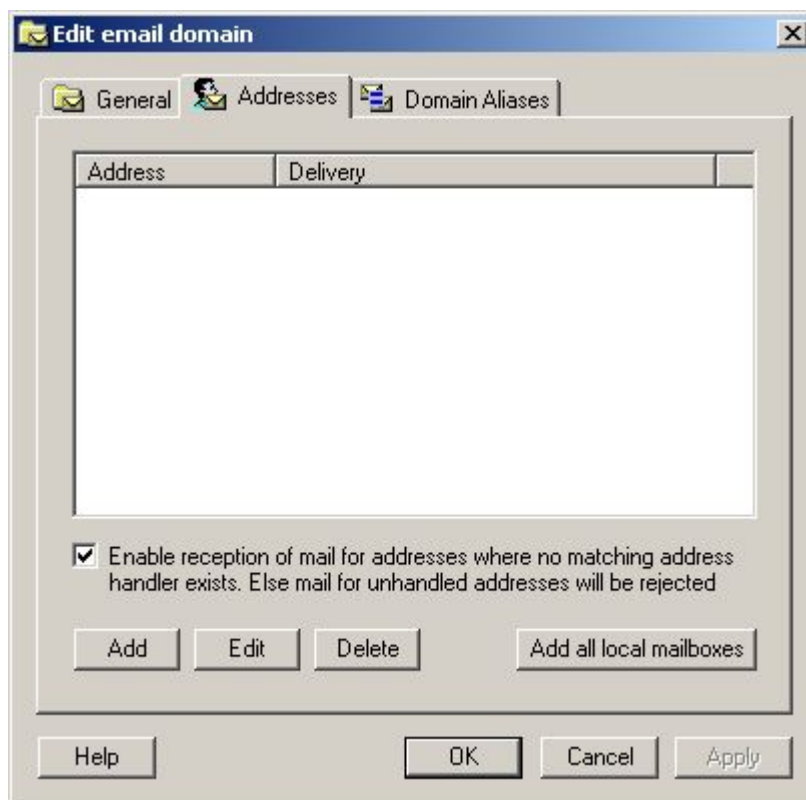
Open the Email properties from the 'System Services' tab in GateKeeper, and the following screen will appear. The domain of the email that is to be hosted now needs to be entered, click Add. (*The Domain you enter needs to have a DNS record located somewhere (either locally by you, or with your service provider)).



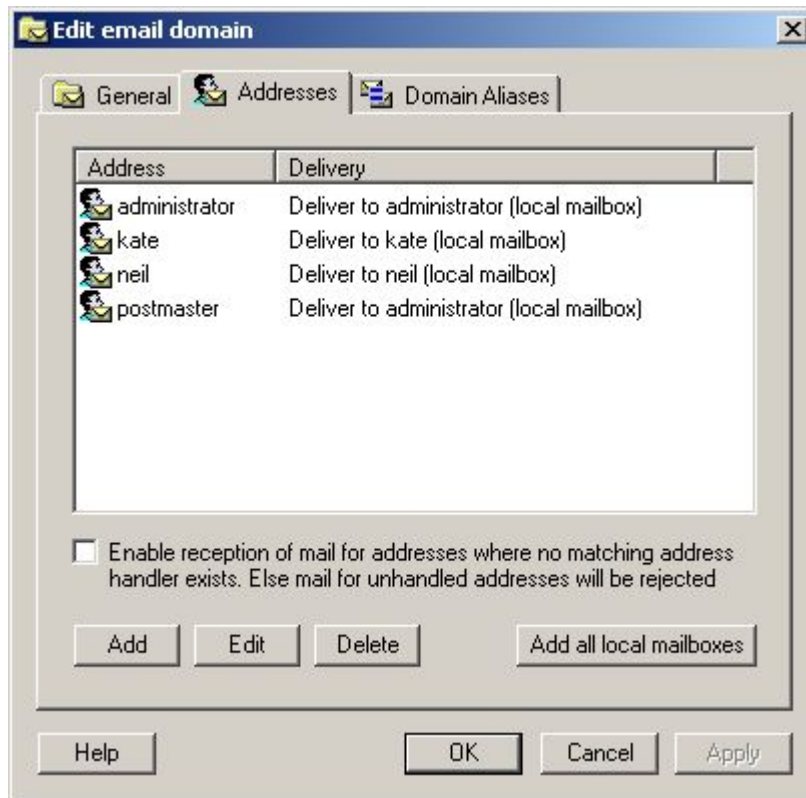
Upon clicking Add the following screen appears, and it is here that Domain specific properties can be set. The General tab indicates whether this new domain is hosted locally or on another server. As WinGate in this scenario, is acting as the primary mail server for the network, 'Mailboxes for this domain are hosted on this server' should be selected.



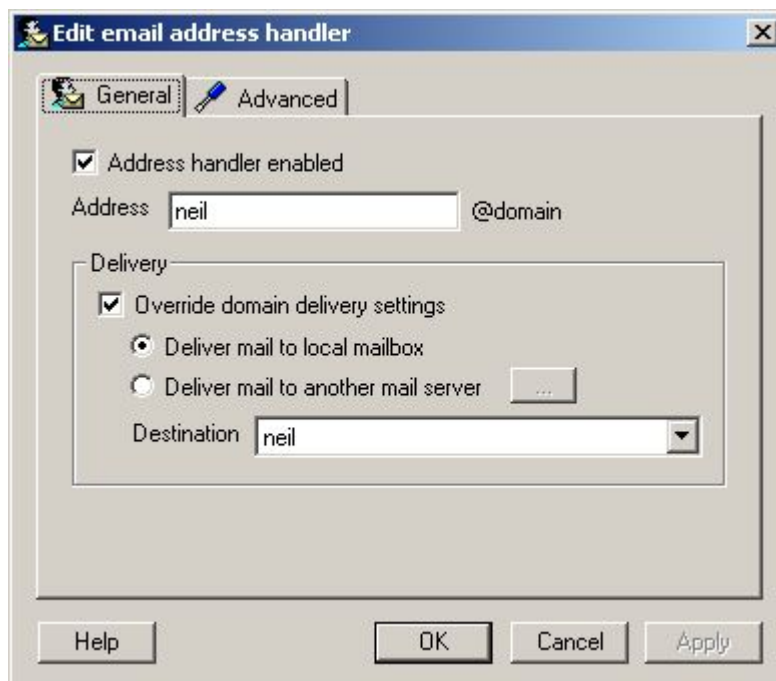
Next email handlers need to be added to the domain, as it is these two pieces of information (the email handler and the domain) that create the email address. An email handler could be a user name that already exists in WinGate or an 'alias' that points to a user within WinGate. There are several ways WinGate mail can deal with these email handlers. By default the screen will appear blank with the option 'To enable reception of mail for addresses where no matching address handler exists' ticked. This setting effectively means that when WinGate receives an email, it will see that there are no email handlers listed, and so will check the user database (be it NT or the WinGate DB) and if a match is found with a user that is enabled for email then the mail will be accepted and delivered, otherwise it will be rejected. So for example, if the user bob has been created as a user in WinGate, and an email is received for bob@qbik.com (presuming that qbik.com is the domain that is being locally hosted), then WinGate will see there is no message handler for bob, but as this option is ticked it will check the user database to see if bob exists there, and as he does, WinGate will accept the email.



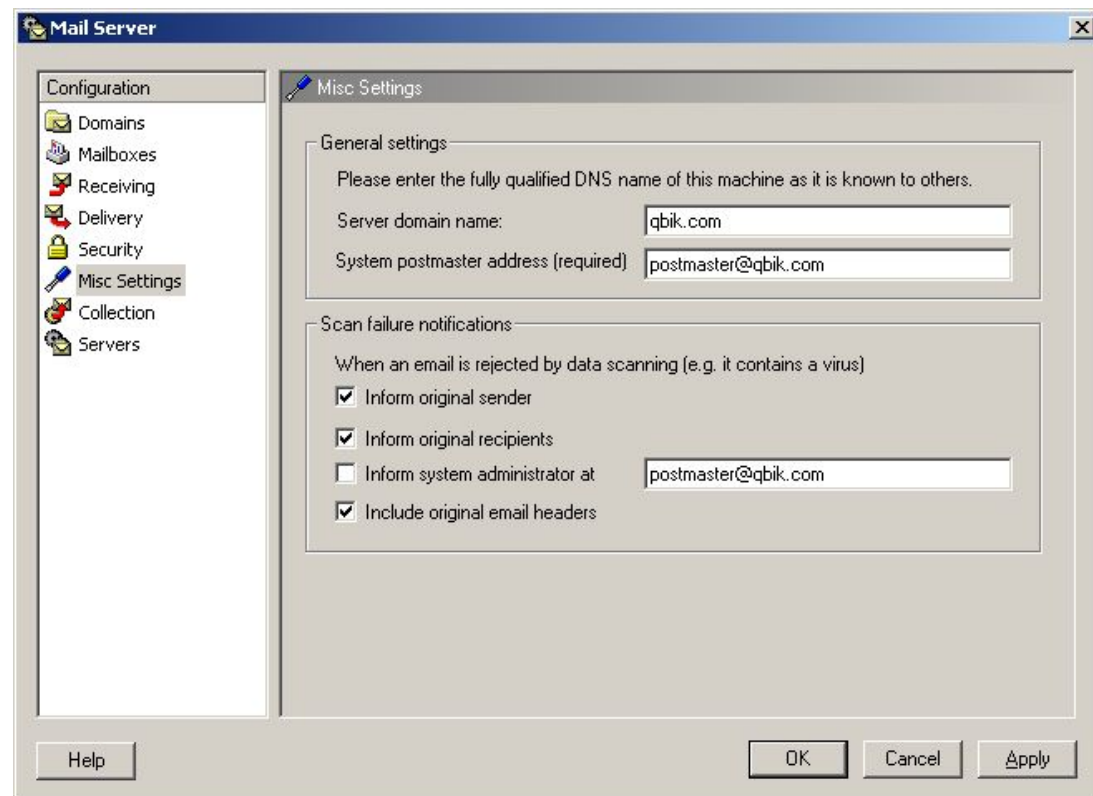
Alternatively, if only specific users will be allowed to receive email for this domain then the 'Enable reception of mail for addresses where no matching address handler exists' should be UNTicked, and specific email handlers added. This can be done in two ways. If all users need to be added them click 'Add all local mailboxes'; otherwise handlers can be added one at a time until all necessary combinations have been covered.



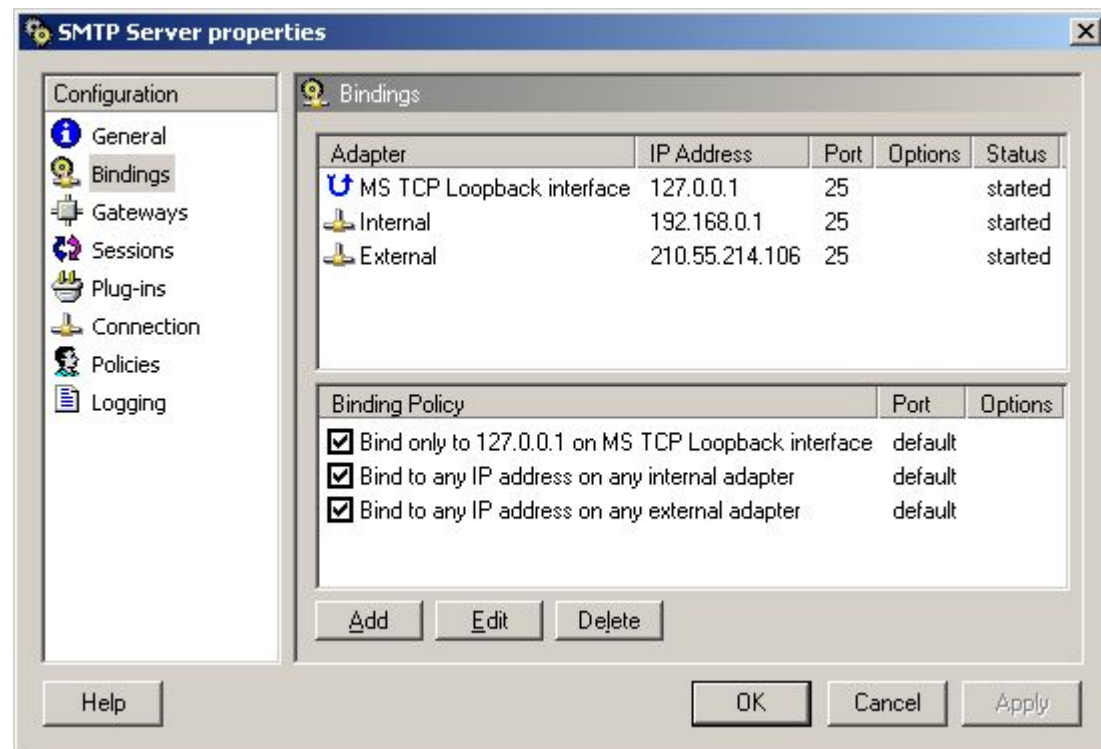
When adding specific email handler overrides there is the option to deliver to a local mailbox (i.e. a local user account) or to specify an alternative destination (email address) with the option of using a different mail server to complete the delivery of this message. In this scenario it is assumed that as WinGate is acting as the primary mail server for the network that all mail will be deliver to local accounts.



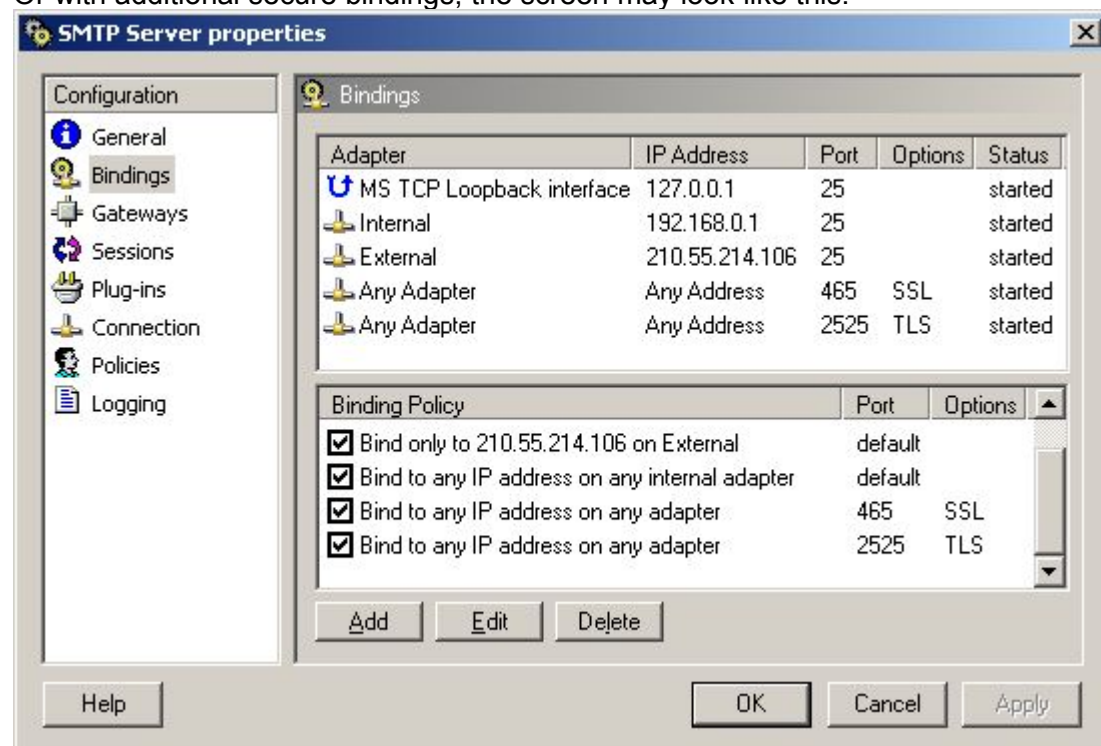
This has now completed the majority of the basic set-up for hosting an email server with WinGate. The defaults for the other options will suffice, except for under the Misc Settings, where the Server Domain Name, and the System Postmaster Address **MUST** be filled out correctly, otherwise mail originating from this server maybe rejected by other mail servers on the internet. The Scan failure notifications configuration is only important if you have Anti Virus for WinGate installed.



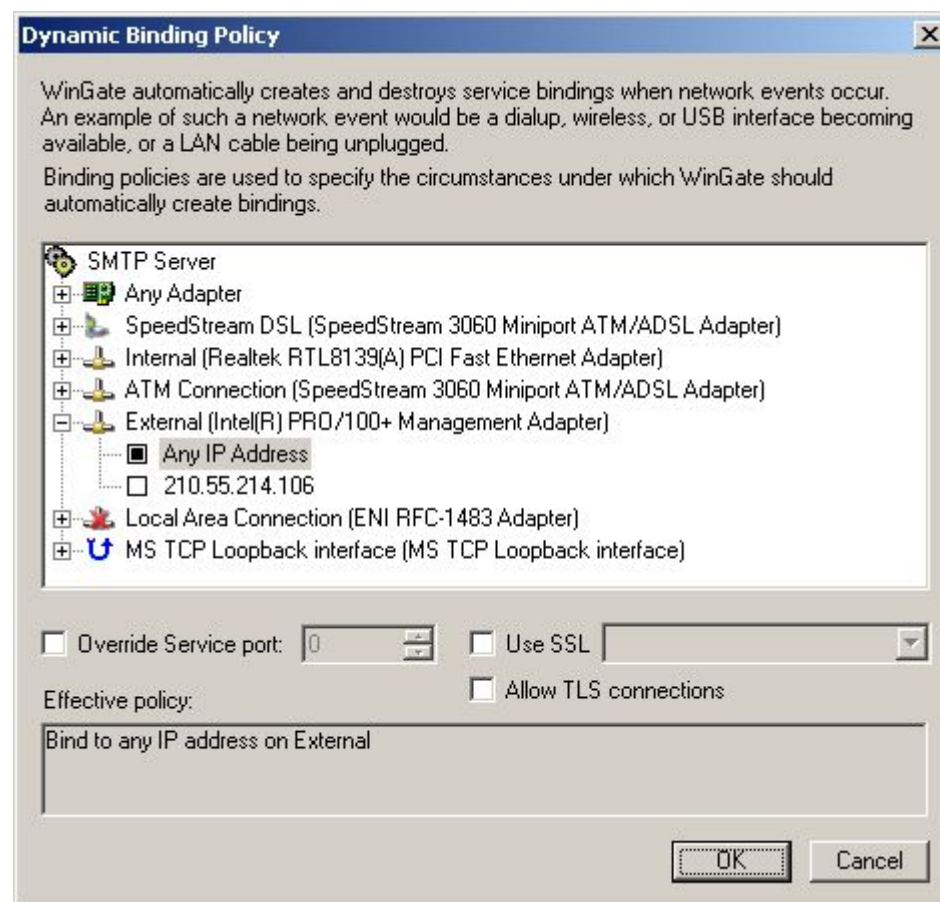
Now that the Server Configuration is complete the only other area of WinGate that needs to be configured are the SMTP bindings. For safety reasons a default install of WinGate only binds services to trusted / internal interfaces, but when setting up WinGate for email, the bindings for SMTP have to be modified so that WinGate can receive emails sent to the domain it is hosting from elsewhere on the internet. From GateKeeper open the SMTP properties on the System tab.



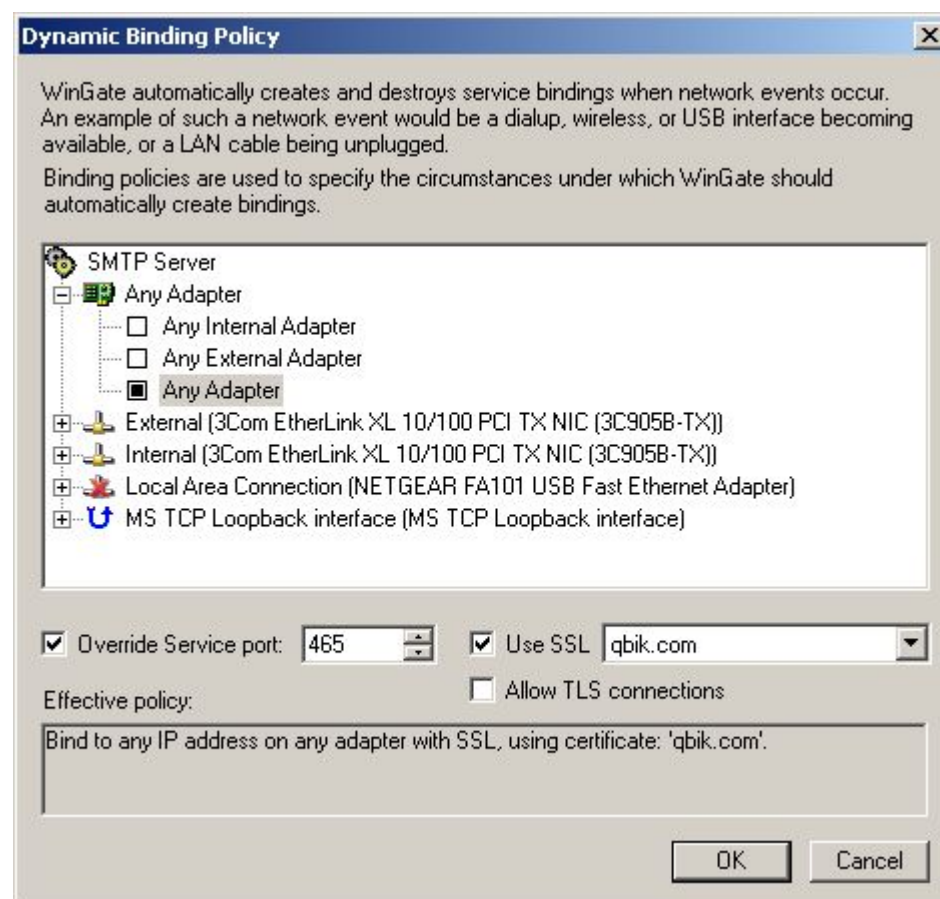
Or with additional secure bindings, the screen may look like this:



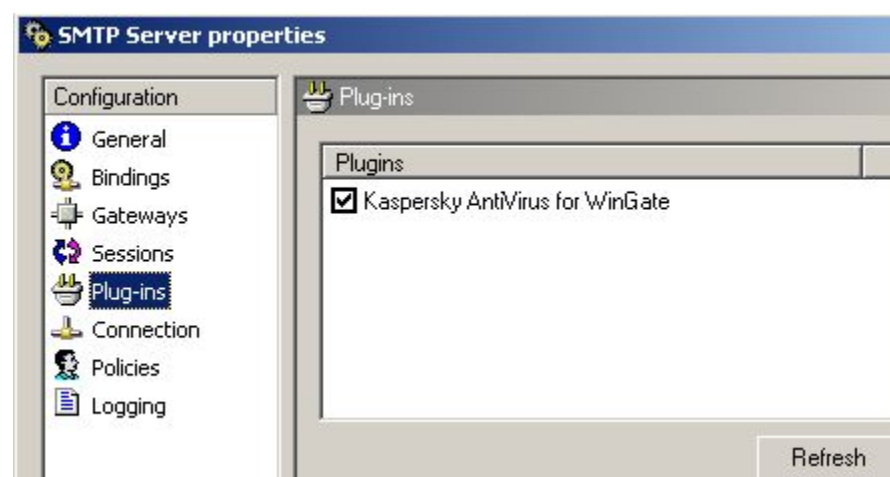
Next click Add to create a new Bindings Policy. For a standard binding, create a new policy for the External adapter for 'Any IP Address'. The other options here are for advanced users so the defaults can be left as they are.




However, to create an advanced bindings policy, in this example using SSL although the same principals apply to TLS, some more options need to be configured. The adapter options can either be set as above, or the option to use 'Any IP' on 'Any Adapter' could be selected as this binding policy will use a different port to any previously configured, and thus there will be no port conflicts. So in addition the Override Service port option should be set to 465, with the Use SSL option ticked, and an appropriate certificate selected. (For more information about Certificates in WinGate see the Help file).



Finally, if you have any WinGate Anti-Virus product installed, check to make sure the Anti-Virus scanning is enabled in the SMTP Server properties.



WinGate is now configured to act as the primary mail server on the network. The next step is to configure the email clients, such as Outlook, Outlook Express, or The Bat etc. These Client machines then need to have their SMTP and Pop3 settings pointed to the WinGate machine's IP address. This example shows the entries that would be made in Outlook Express if the WinGate server's IP was 192.168.0.100.



The image shows a screenshot of the 'WinGate Mail Properties' dialog box. It has four tabs: 'General', 'Servers', 'Connection', and 'Advanced'. The 'General' tab is selected. The 'Server Information' section contains two text boxes: 'Incoming mail (POP3):' with the value '192.168.0.100' and 'Outgoing mail (SMTP):' with the value '192.168.0.100'. The 'Incoming Mail Server' section contains an 'Account name:' text box with 'neil', a 'Password:' text box with 'xxxxxxxx', a checked 'Remember password' checkbox, and an unchecked 'Log on using Secure Password Authentication' checkbox. The 'Outgoing Mail Server' section contains an unchecked 'My server requires authentication' checkbox and a 'Settings...' button. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

WinGate Mail Properties

General Servers Connection Advanced

Server Information

Incoming mail (POP3): 192.168.0.100

Outgoing mail (SMTP): 192.168.0.100

Incoming Mail Server

Account name: neil

Password: xxxxxxxx

☒ Remember password

☐ Log on using Secure Password Authentication

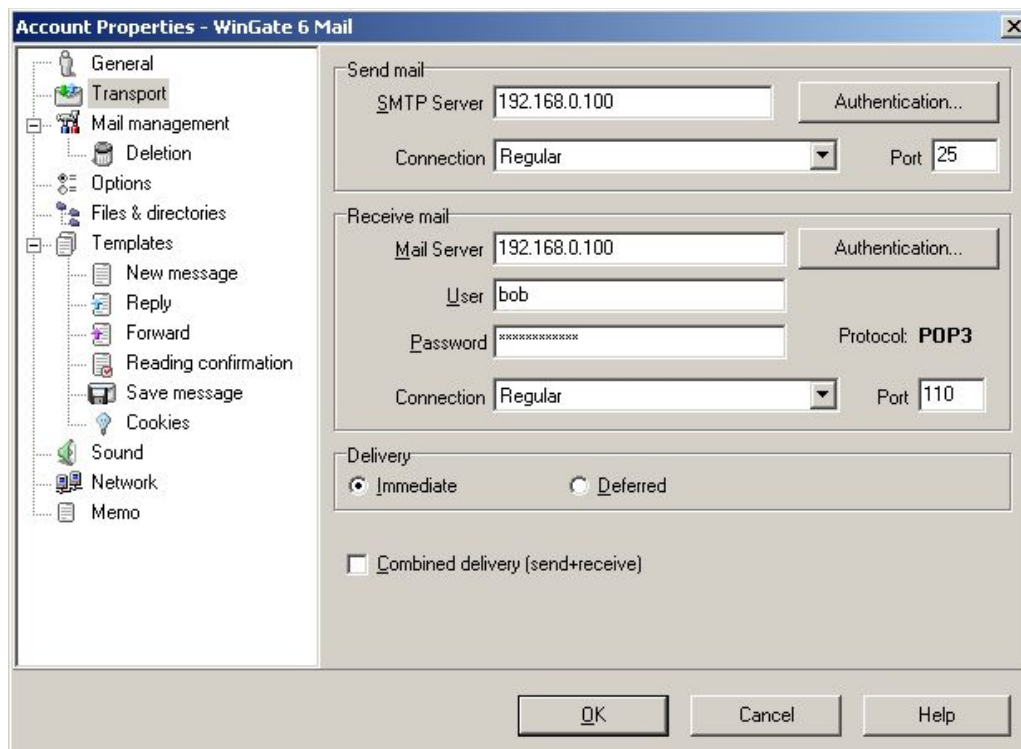
Outgoing Mail Server

☐ My server requires authentication

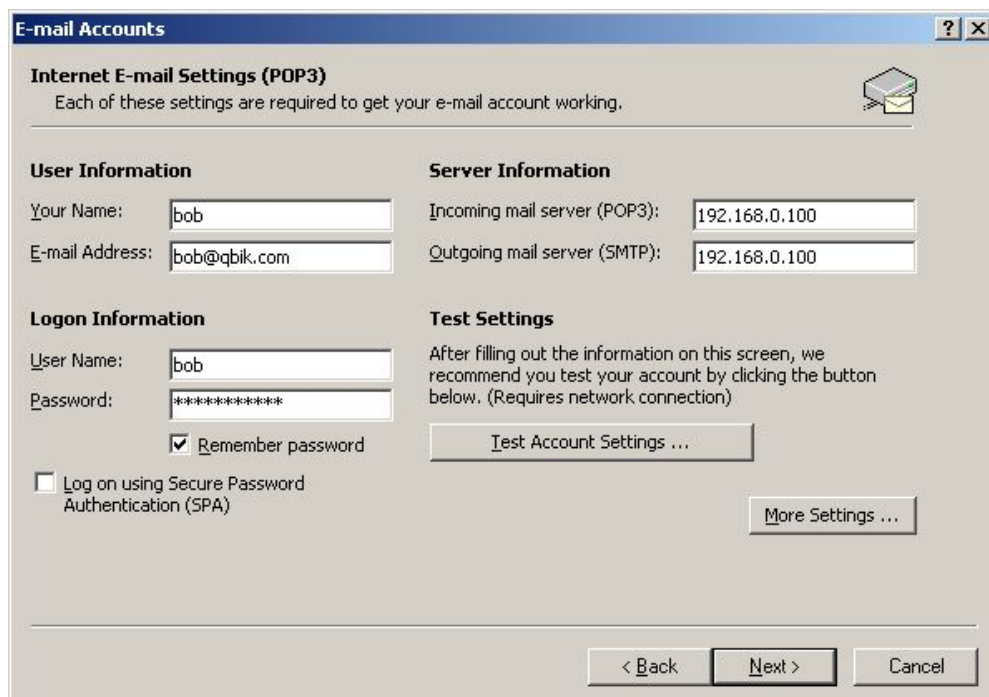
Settings...

OK Cancel Apply

This example shows how The Bat mail client would be configured if the WinGate server's IP was 192.168.0.100.

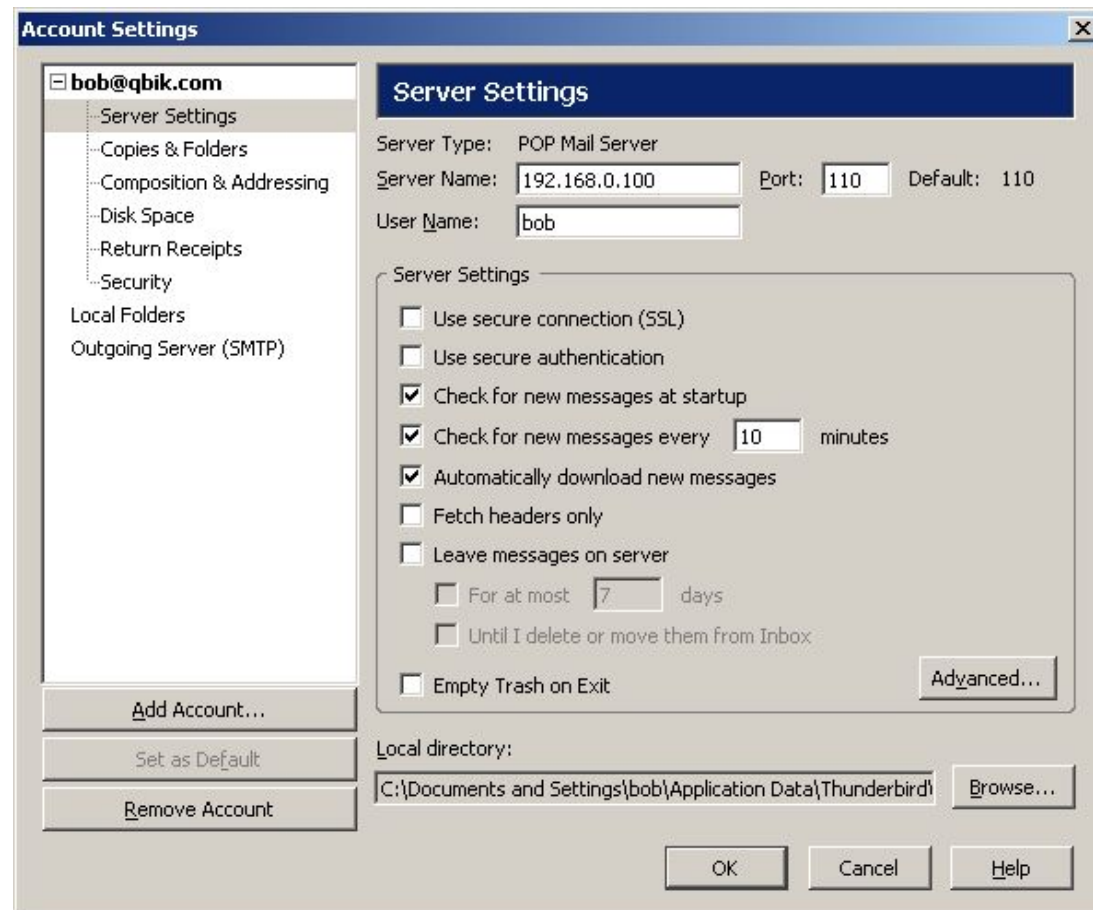


This example shows how Outlook XP mail client would be configured if the WinGate server's IP was 192.168.0.100.

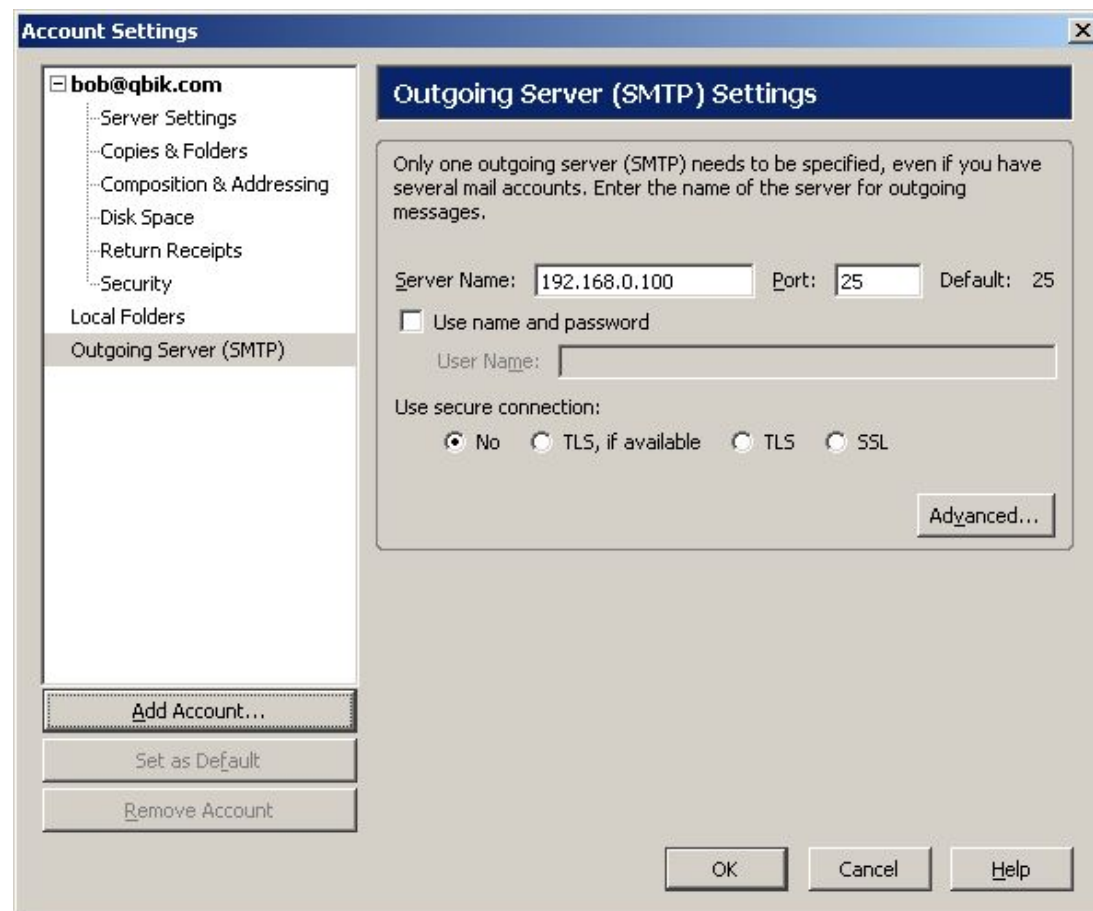


This example shows how the ThunderBird mail client would be configured if the WinGate server's IP was 192.168.0.100.

Firstly POP3:

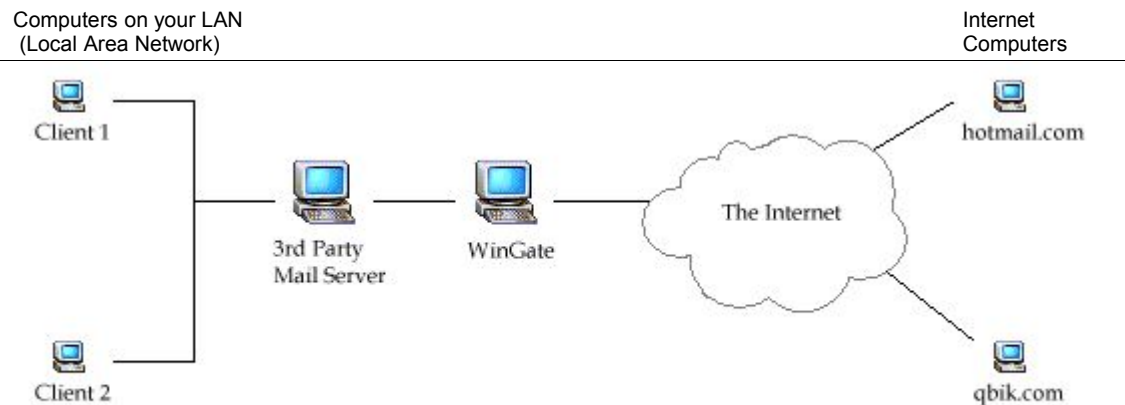


Then SMTP:



Scenario 2:

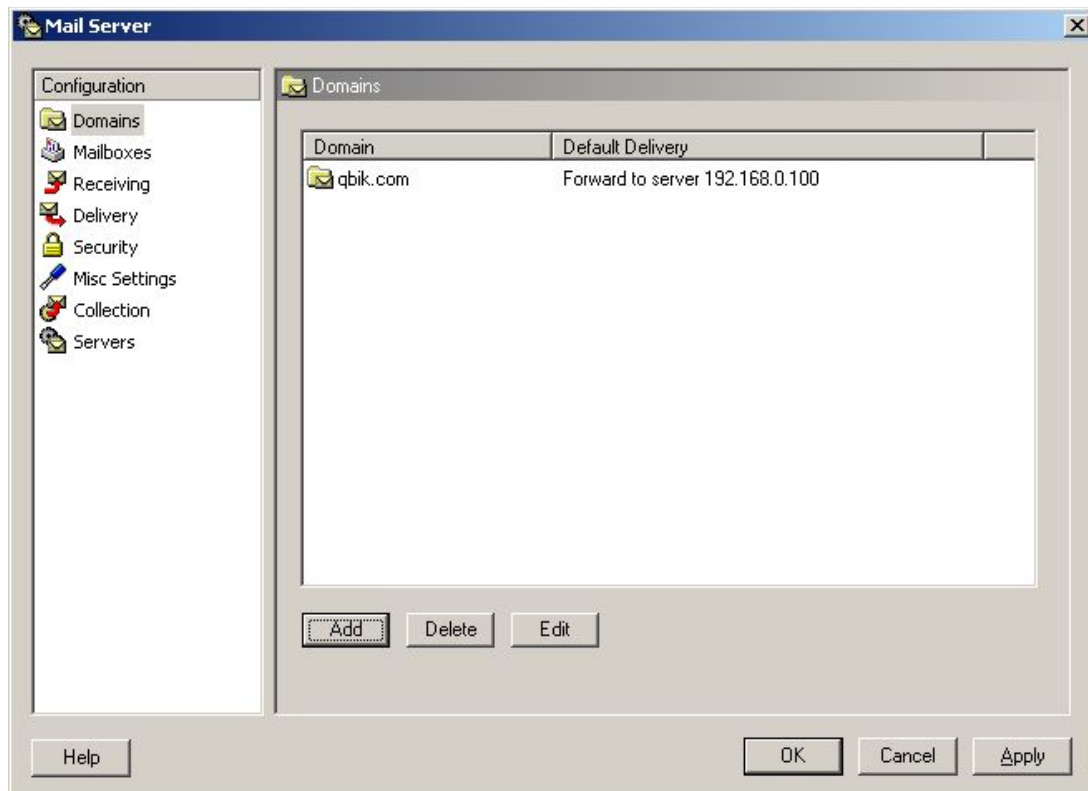
A mail server already exists on the network:



In this situation a 3rd party standalone mail server is responsible for looking after email on your network. There are actually two ways that this situation could be set up. The 3rd party mail server could either be configured to deliver its mail to the WinGate mail server which then delivers this email out to the internet, or the 3rd party mail server could 'pass through' WinGate and deliver the email directly itself. We would recommend that you still use WinGate's mail server in this chain as this then gives the added safety of WinGate's Anti-Virus. This section will detail how WinGate needs to be configured to get both situations working.

1) If you choose to configure your 3rd party mail server to deliver to WinGate, and then out on to the internet.

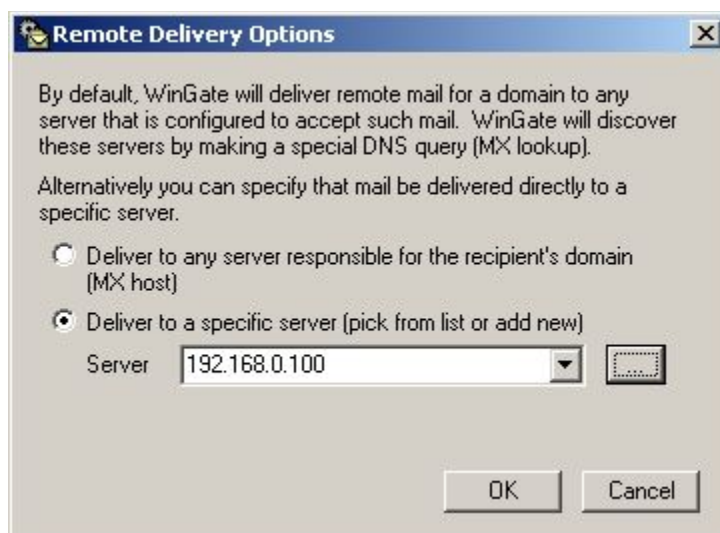
Open the Email properties from the 'System Services' tab in GateKeeper and, under the Domains option, click Add. Enter the name of the domain that is hosted on by the 3rd party mail server. Here it is qbik.com. Even though WinGate isn't hosting the domain it still needs to know what your domain is so that it is able to pass the correct email along to the 3rd party mail server. (*The Domain you enter needs to have a DNS record located somewhere (either locally by you, or with your service provider)).



Once the Domain name has been entered, WinGate then needs to be told that it isn't the primary mail server for the network, so move the radio button to 'Mailboxes for this domain are hosted on another server', and click the '...' button at the end of the line.



This is where the IP of the 3rd party mail server's IP needs to be entered. Put the radio button next to 'Deliver to a specific server' and type the IP in the space provided (in this case its 192.168.0.100)



If this 3rd party mail server is listening on a different port to the standard one(25), or needs any special kind of connection (i.e. authentication etc) then click the '...' button to add these options.

Server Properties

General

Server: 192.168.0.100 Port: 25

Description: Internal LAN mail server

Security

☒ Use secure connection if supported by server (TLS)

☐ Server requires authentication

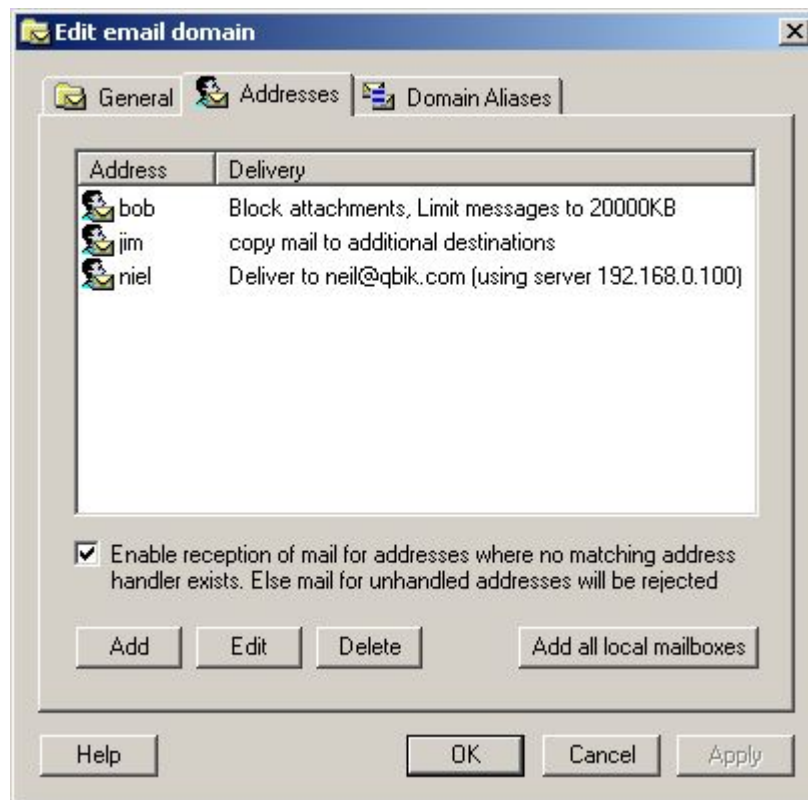
Username:

Password:

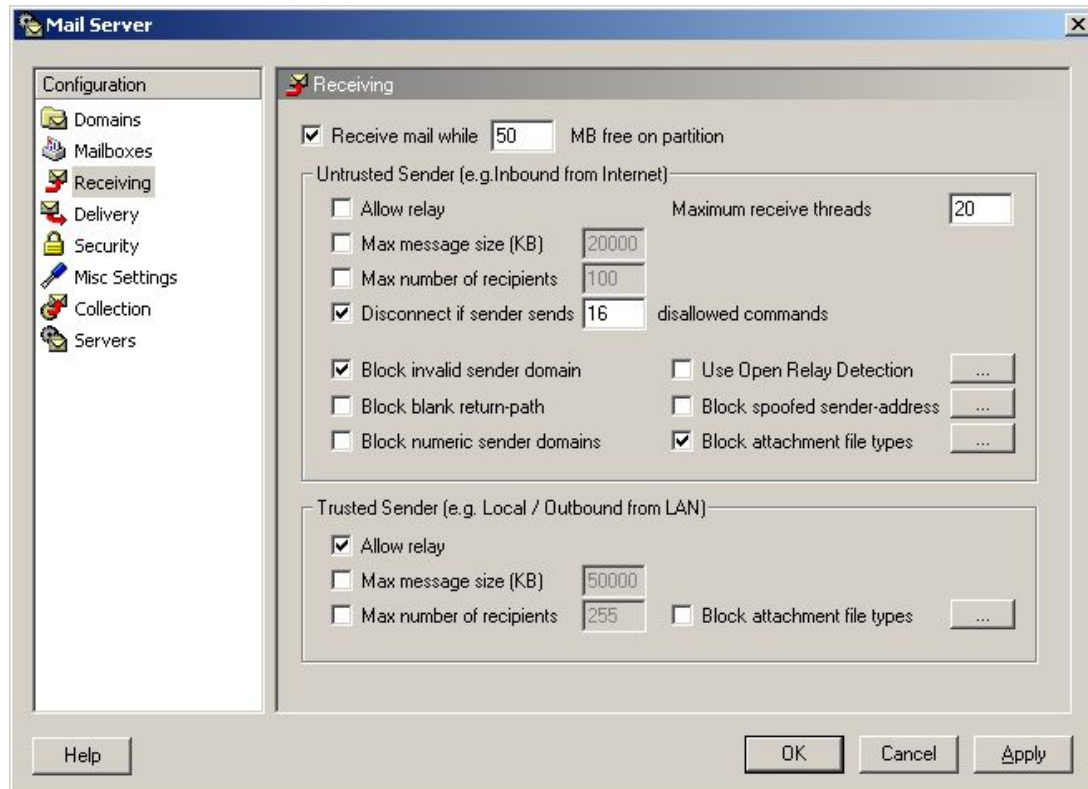
Method: use best method available

OK Cancel

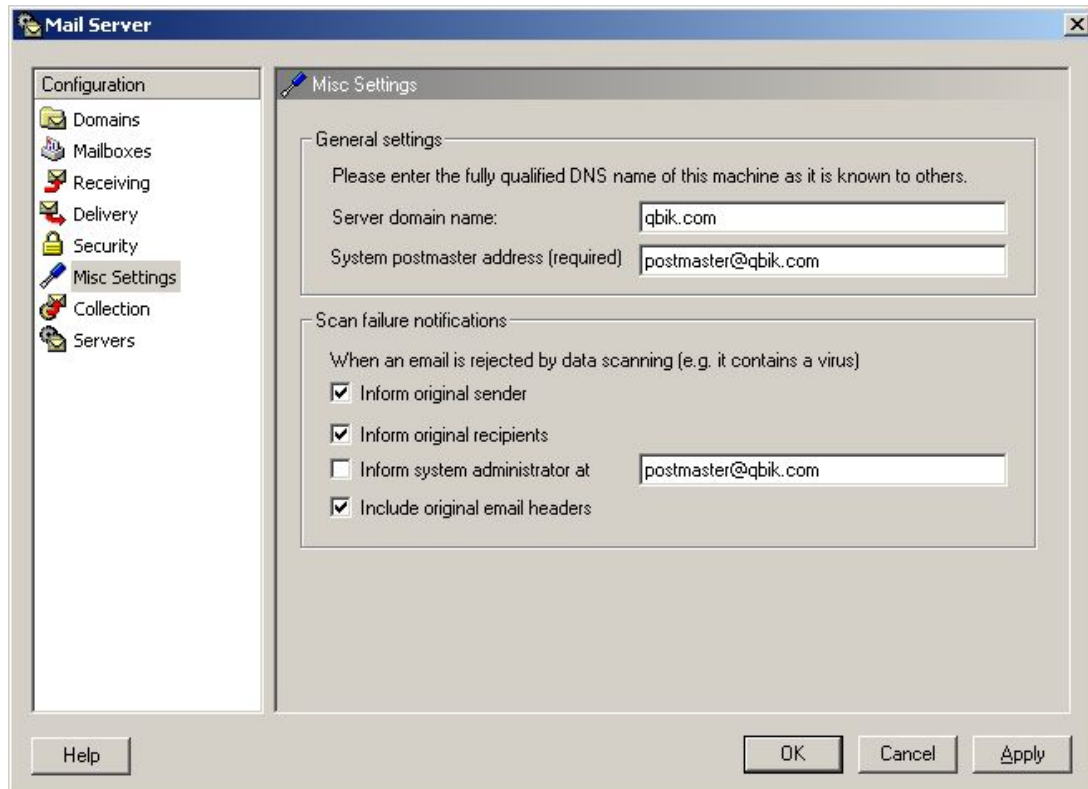
Back on the Edit Email Domain properties, under the addresses tab, there are two ways to configure the email handlers. If the 3rd party email server is to decide which accounts / addresses to accept mail for then the default option (Enable reception of mail for addresses where no matching address handler exists) should be left ticked. However, if specific overrides are required, then they can be added here instead of / as well as the default reception option.



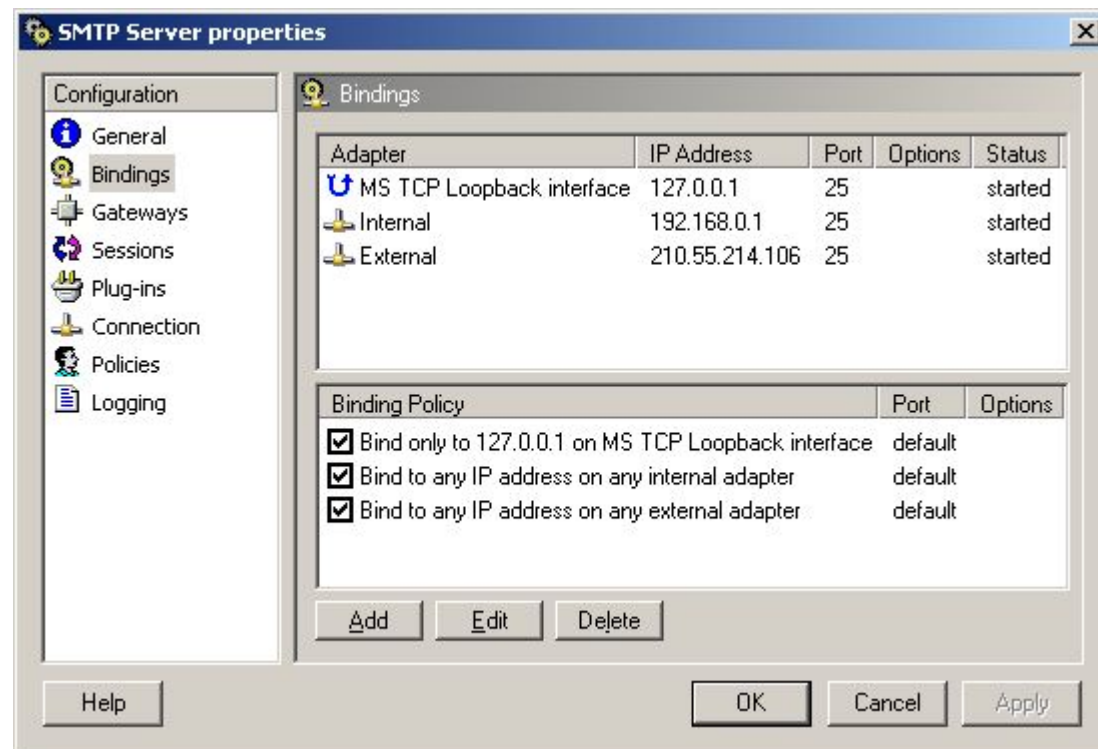
Click OK on this Edit email domains dialog. This has now completed the majority of the basic set-up for hosting an 3rd party email server behind WinGate. The default settings for Receiving do not need to be changed, although can be tweaked if required.



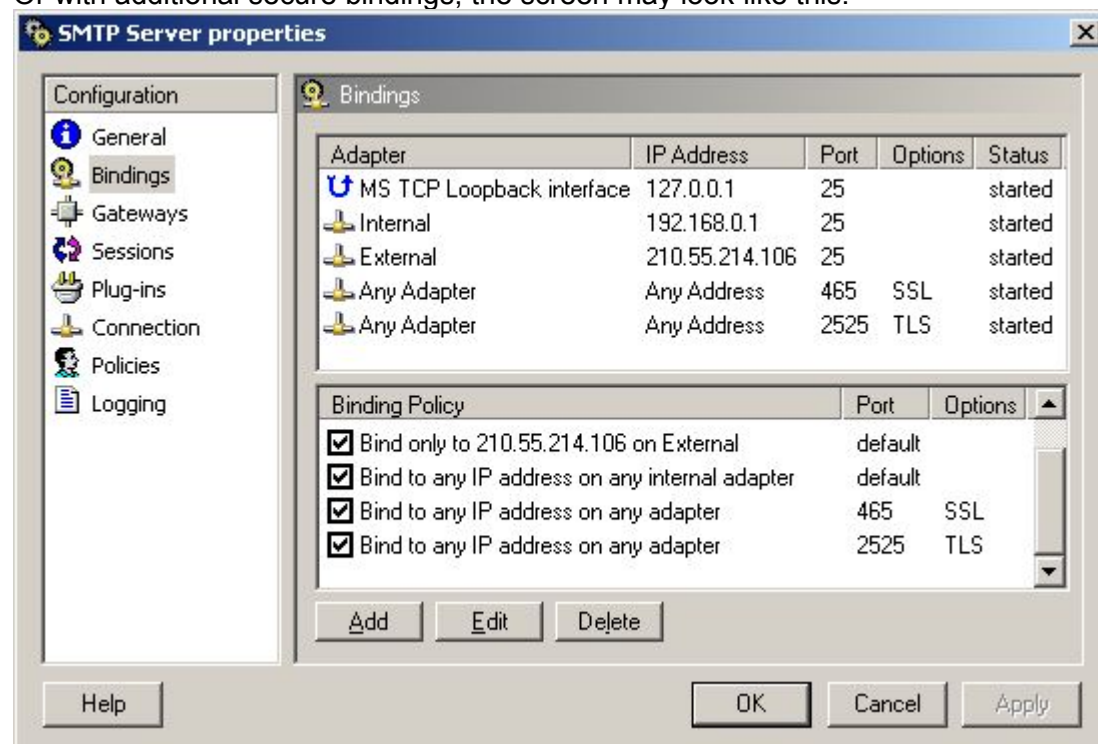
Under the Misc Settings, the Server Domain Name, and the System Postmaster Address MUST be filled out correctly, otherwise mail originating from this server maybe rejected by other mail servers on the internet. This is important in this scenario as the 3rd party mail server will send to WinGate and then WinGate will deliver to the outside world, and thus it will be WinGate that identifies this domain to other servers. The Scan failure notifications configuration is only important if you have Anti Virus for WinGate installed.



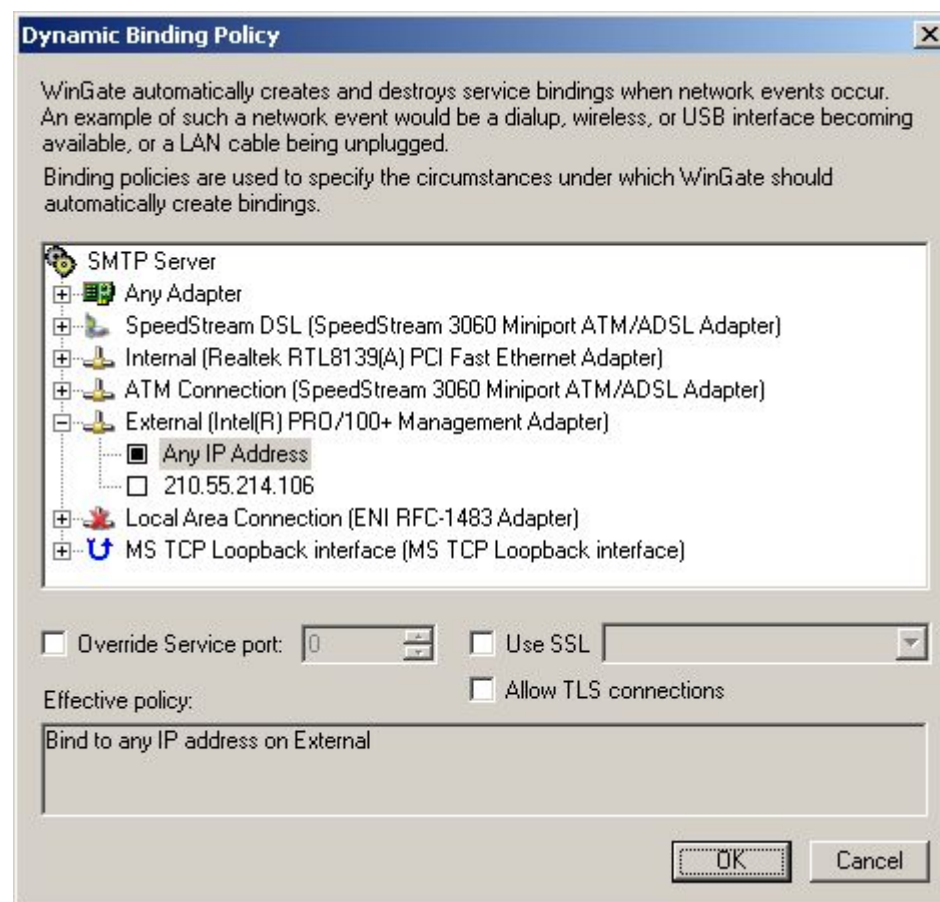
Now that the Server Configuration is complete the only other area of WinGate that needs to be configured are the SMTP bindings. For safety reasons a default install of WinGate only binds services to trusted / internal interfaces, but when setting up WinGate for email, the bindings for SMTP have to be modified so that WinGate can receive emails sent to the domain it is hosting from elsewhere on the internet. From GateKeeper open the SMTP properties on the System tab.



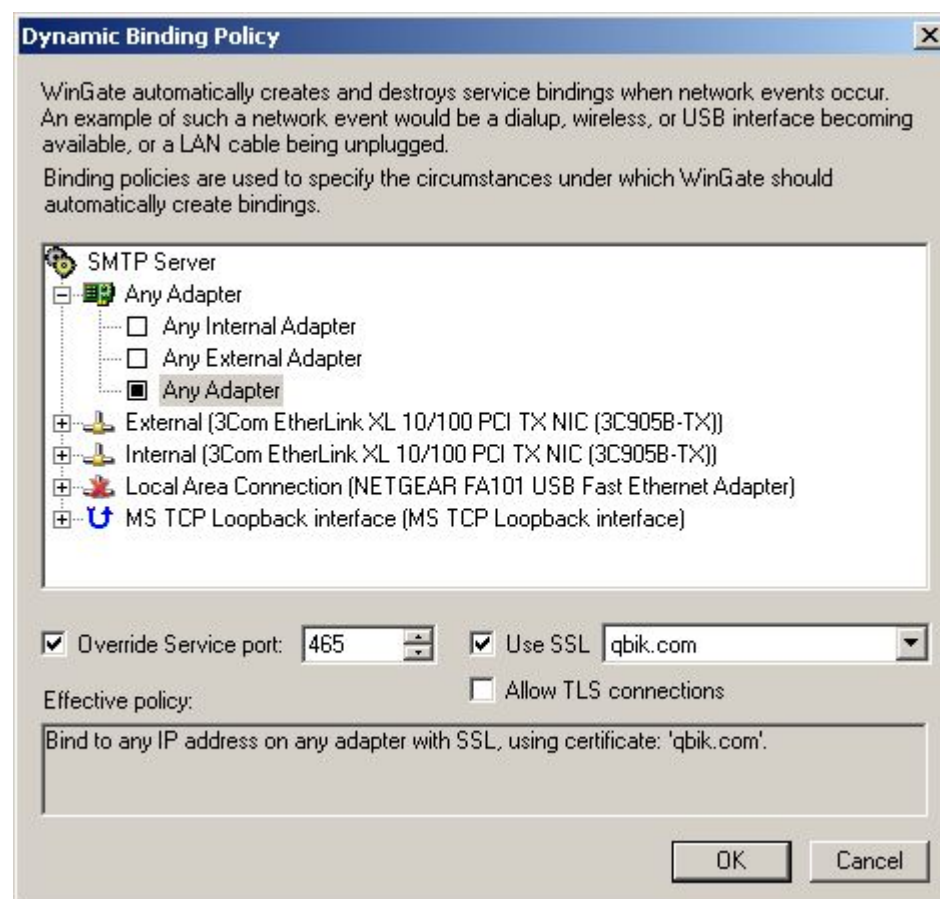
Or with additional secure bindings, the screen may look like this:



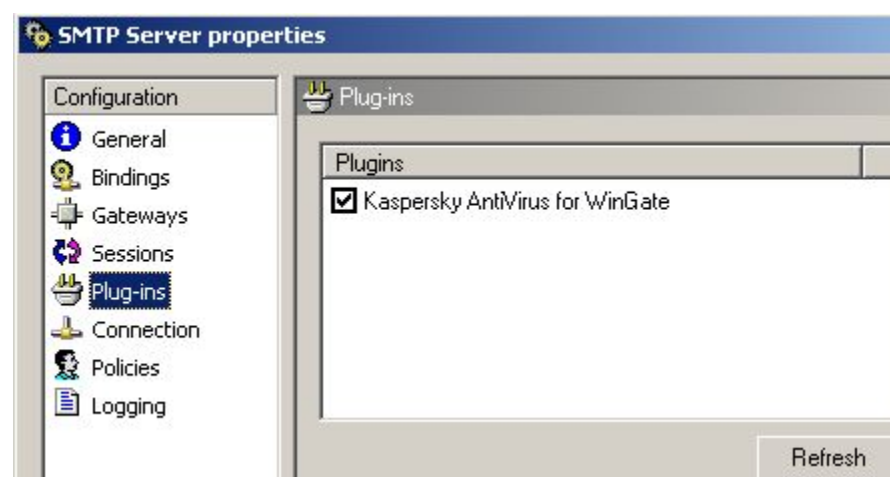
Next click Add to create a new Bindings Policy. For a standard binding, create a new policy for the External adapter for 'Any IP Address'. The other options here are for advanced users so the defaults can be left as they are.



However, to create an advanced bindings policy, in this example using SSL although the same principals apply to TLS, some more options need to be configured. The adapter options can either be set as above, or the option to use 'Any IP' on 'Any Adapter' could be selected as this binding policy will use a different port to any previously configured, and thus there will be no port conflicts. So in addition the Override Service port option should be set to 465, with the Use SSL option ticked, and an appropriate certificate selected. (For more information about Certificates in WinGate see the Help file).

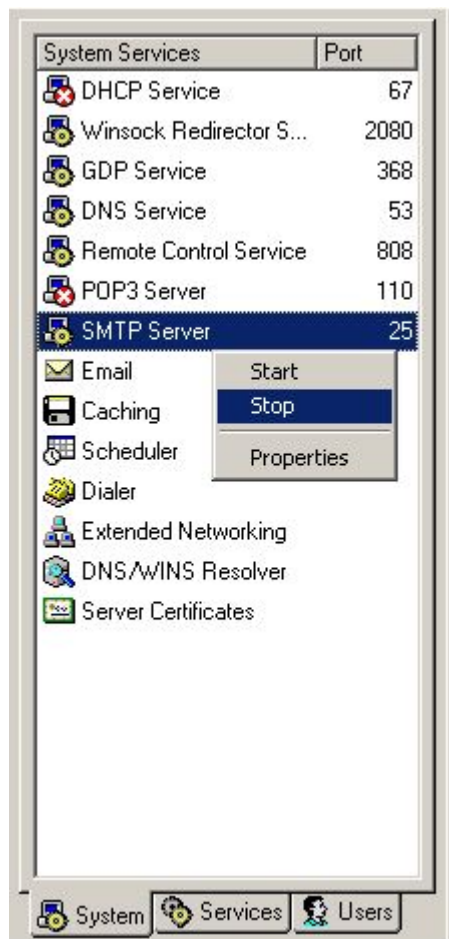


Finally, if you have any WinGate Anti-Virus product installed, check to make sure the Anti-Virus scanning is enabled in the SMTP Server properties.

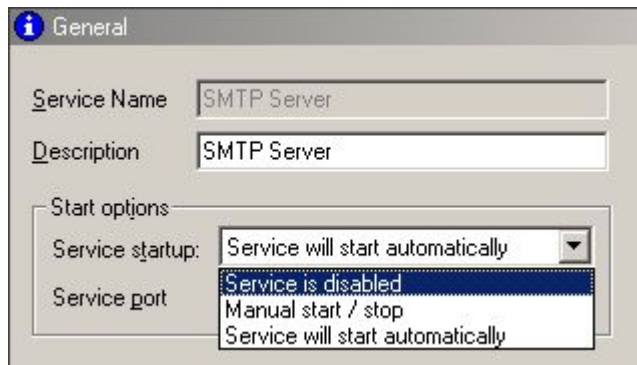


2) If it would be preferable to have the 3rd party mail server simply 'pass through' WinGate and receive and deliver the mail directly to the internet, then WinGate needs to be additionally configured as follows (This description presumes the ENS is installed):

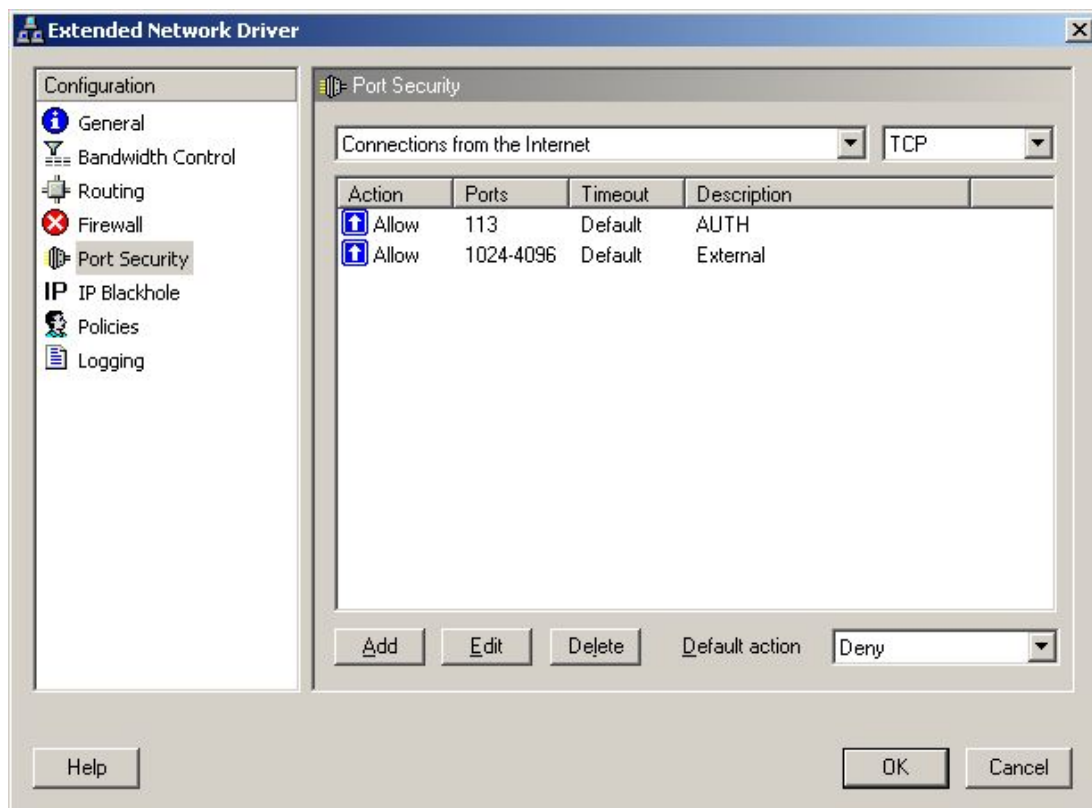
As none of WinGate's specific mail functions will be used, these will need to be switched off, to stop them interfering when mail is trying to 'pass through'. To do this, right click on both the POP3 and SMTP Servers in the System Services tab and select Stop.



Each service then needs to be modified so that it will not restart again if the WinGate engine is restarted. To do this, bring up the properties window for both the SMTP and POP server (one at a time) by right clicking on the service. Then from the Service Start-up drop down list on the General pane, select Service is disabled.



To ensure mail sent to your domain gets through to the 3rd party mail server, a redirect needs to be added so that WinGate knows where to forward the inbound email onto. This is done in the ENS properties via the Port Security pane.



Click Add, and fill out the port redirection as follows (where 192.168.0.100 is the IP address of the 3rd party mail server). This needs to be done individually for SMTP (port 25) and POP (port 110).

Port Range Configuration

Port range specification

Description: Inbound SMTP re-direct to 3rd party mail server on LAN

☒ Internet computers to the WinGate PC ☒ ICP
☐ Internet computers to DMZ ☐ UDP
☐ Local computers to the WinGate PC
☐ Local computers to the internet
☐ DMZ computers to the WinGate PC

Ports: 25 to 25

Action

☐ Allow Packet
☐ Drop Packet
☒ Redirect Packet to IP address: 192.168.0.100
☐ Dont translate source IP ☐ Override port: 1

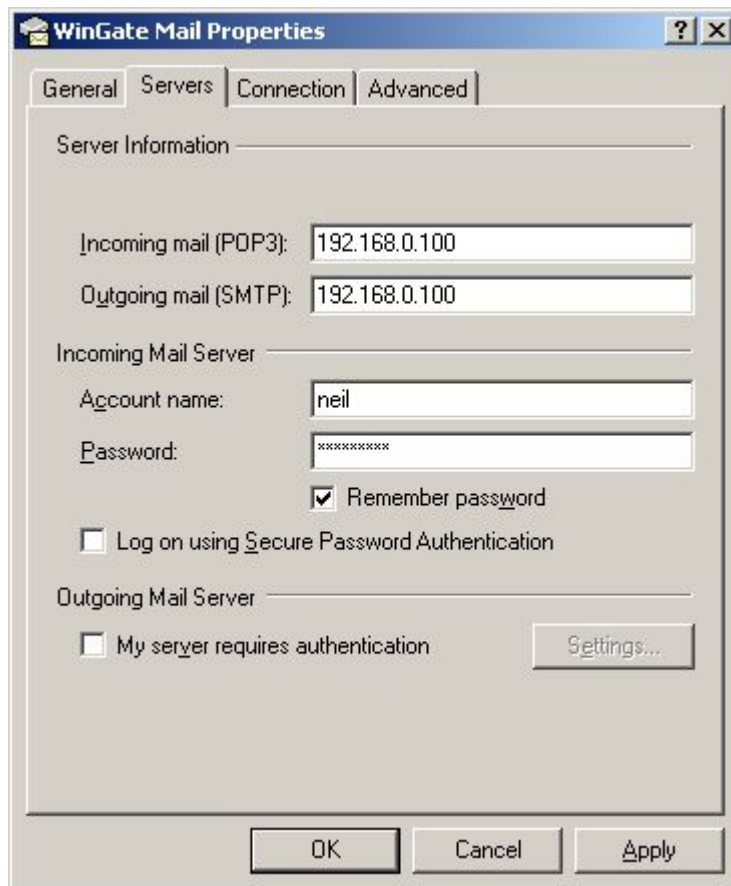
Options

☒ Use SYN cookies ☒ Use default timeouts
☐ Notify on access ☐ Never timeout
☒ Cloak connection failures ☐ Timeout in: 0 sec

OK Cancel

WinGate doesn't require any configuration to send email as the 3rd party mail server should be configured to use WinGate as it's default gateway, and thus will use NAT to connect to the internet.

Irrespective of whether you have WinGate in pass through or forwarding mode, client computers should have their Mail clients set up identically to send and receive. This example shows the entries that would be made in Outlook Express if the 3rd party mail Server's IP was 192.168.0.100



The image shows the 'WinGate Mail Properties' dialog box with the 'General' tab selected. The 'Server Information' section contains two text boxes: 'Incoming mail (POP3):' with the value '192.168.0.100' and 'Outgoing mail (SMTP):' with the value '192.168.0.100'. The 'Incoming Mail Server' section includes a text box for 'Account name:' with the value 'neil', a text box for 'Password:' with the value 'xxxxxxxx', a checked checkbox for 'Remember password', and an unchecked checkbox for 'Log on using Secure Password Authentication'. The 'Outgoing Mail Server' section has an unchecked checkbox for 'My server requires authentication' and a 'Settings...' button. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

WinGate Mail Properties

General Servers Connection Advanced

Server Information

Incoming mail (POP3): 192.168.0.100

Outgoing mail (SMTP): 192.168.0.100

Incoming Mail Server

Account name: neil

Password: xxxxxxxx

☒ Remember password

☐ Log on using Secure Password Authentication

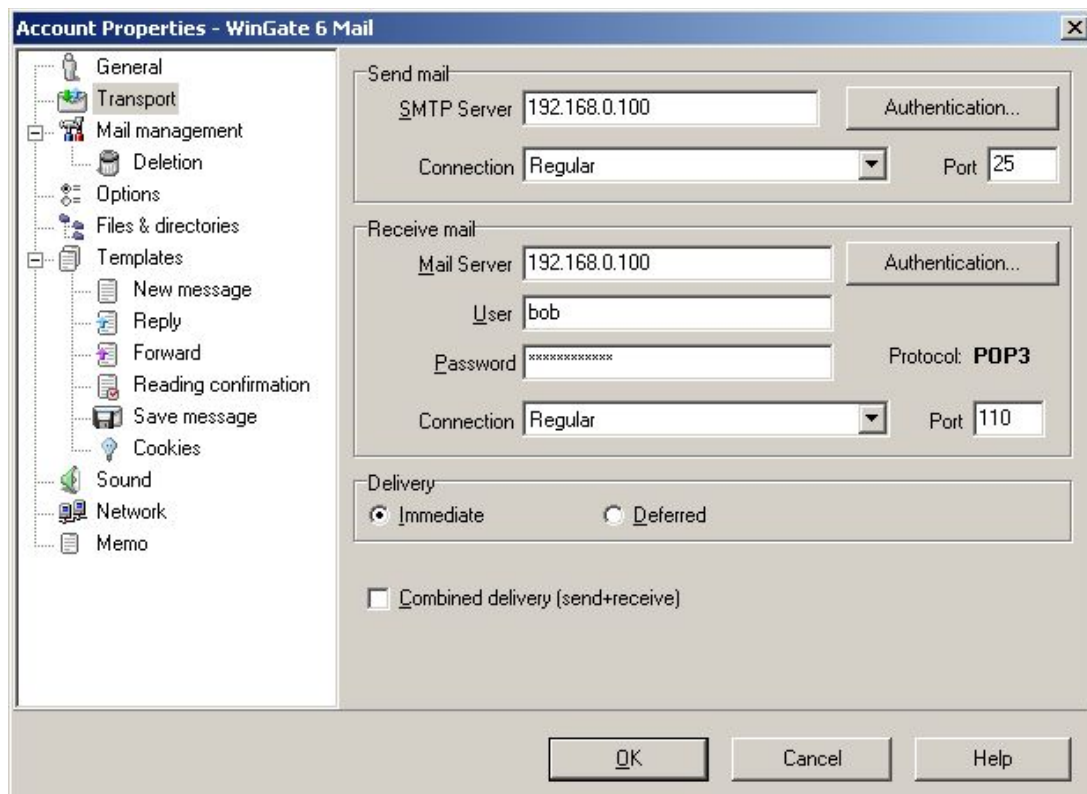
Outgoing Mail Server

☐ My server requires authentication

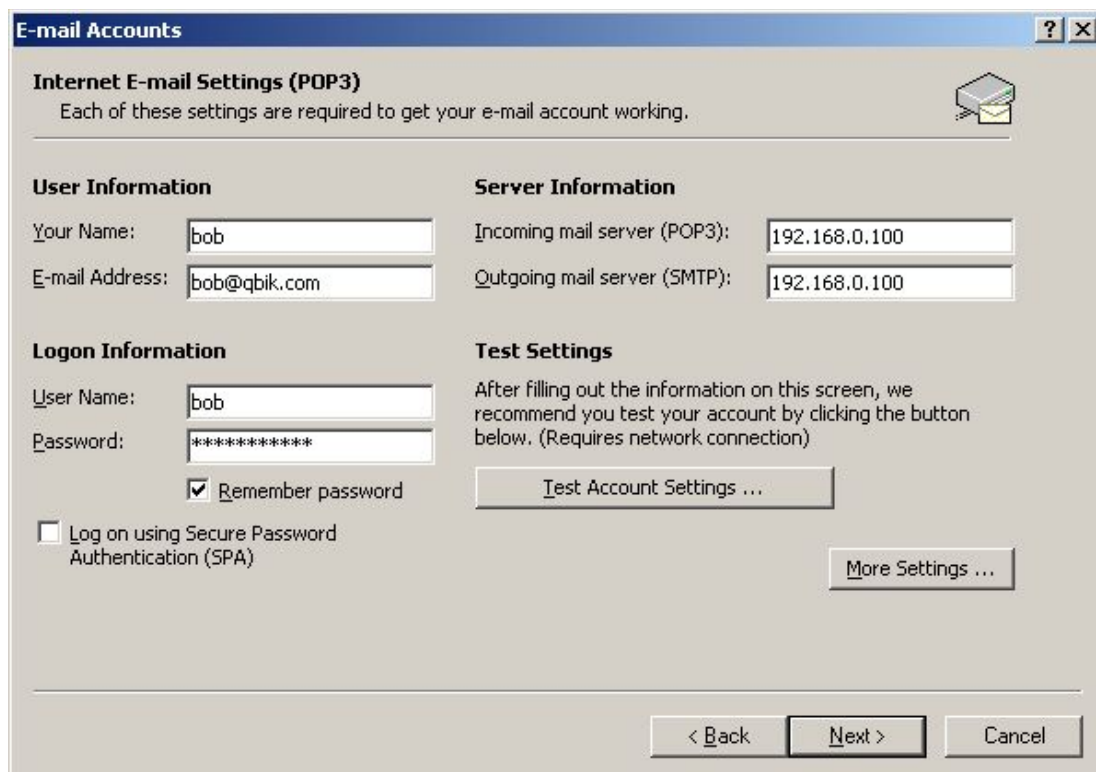
Settings...

OK Cancel Apply

This example shows how The Bat would be configured if the 3rd party mail server's IP was 192.168.0.100

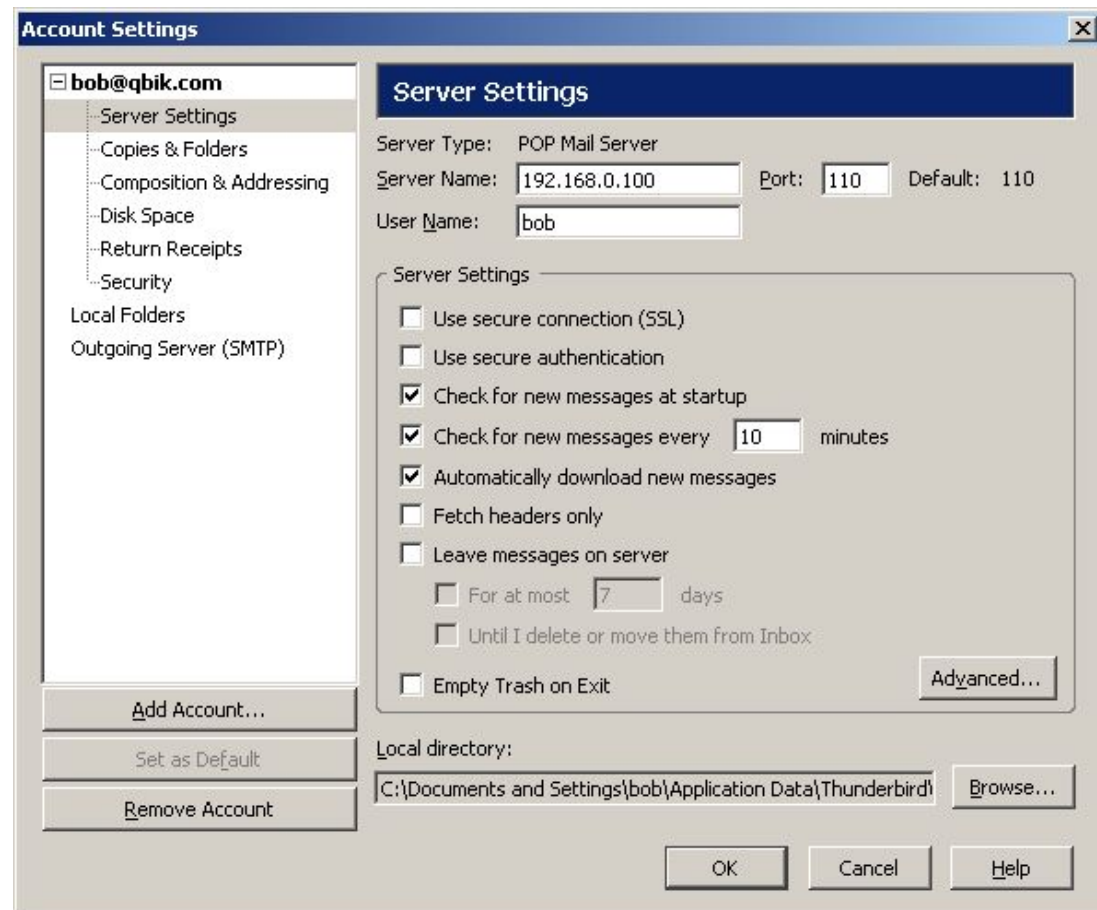


This example shows how Outlook XP would be configured if the 3rd party mail server's IP was 192.168.0.100

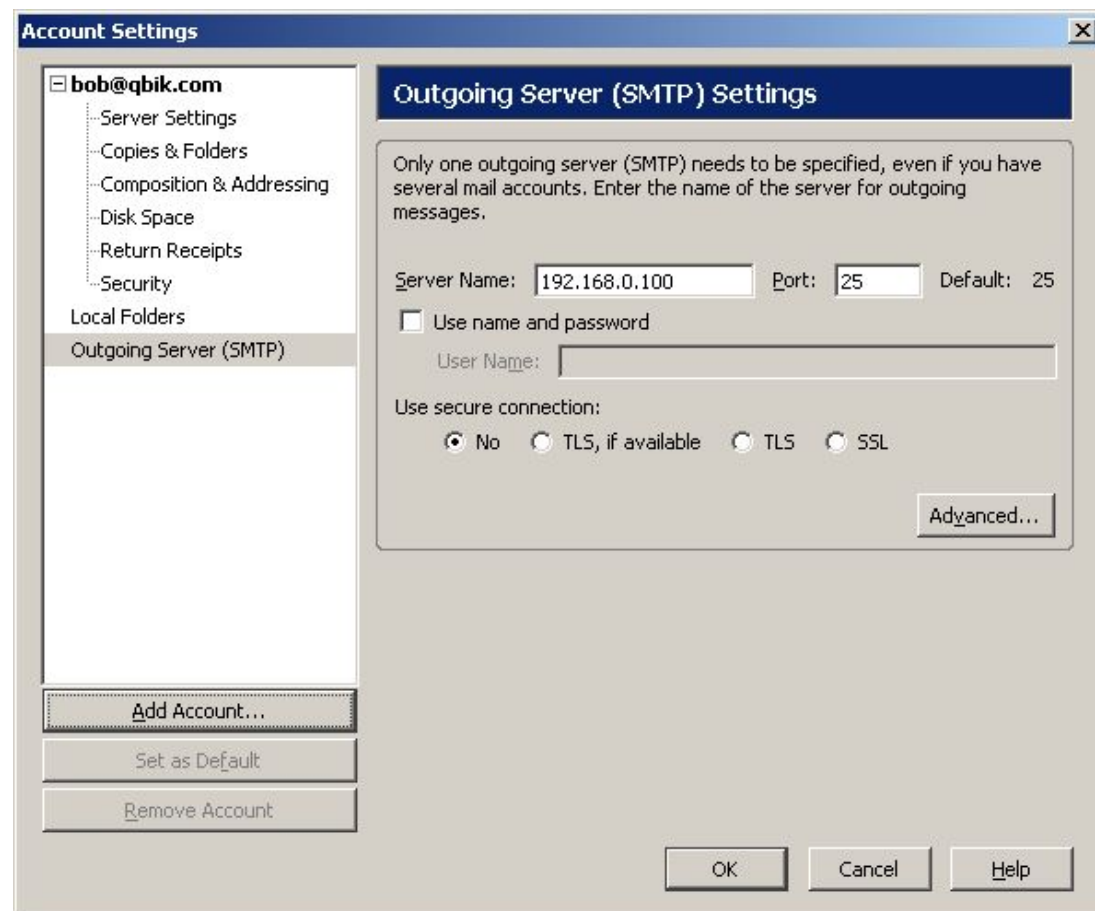


This example shows how Thunderbird would be configured if the 3rd party mail server's IP was 192.168.0.100

Firstly POP3:



Then SMTP:

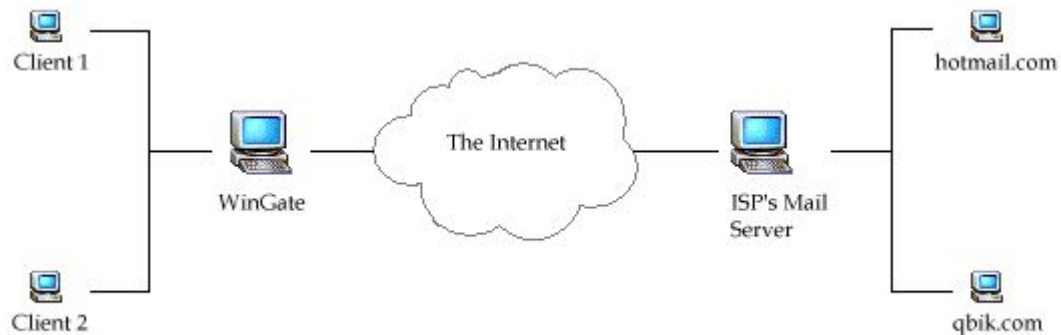


Scenario 3:

An ISP hosts mail for the domain

Computers on your
LAN
(Local Area Network)

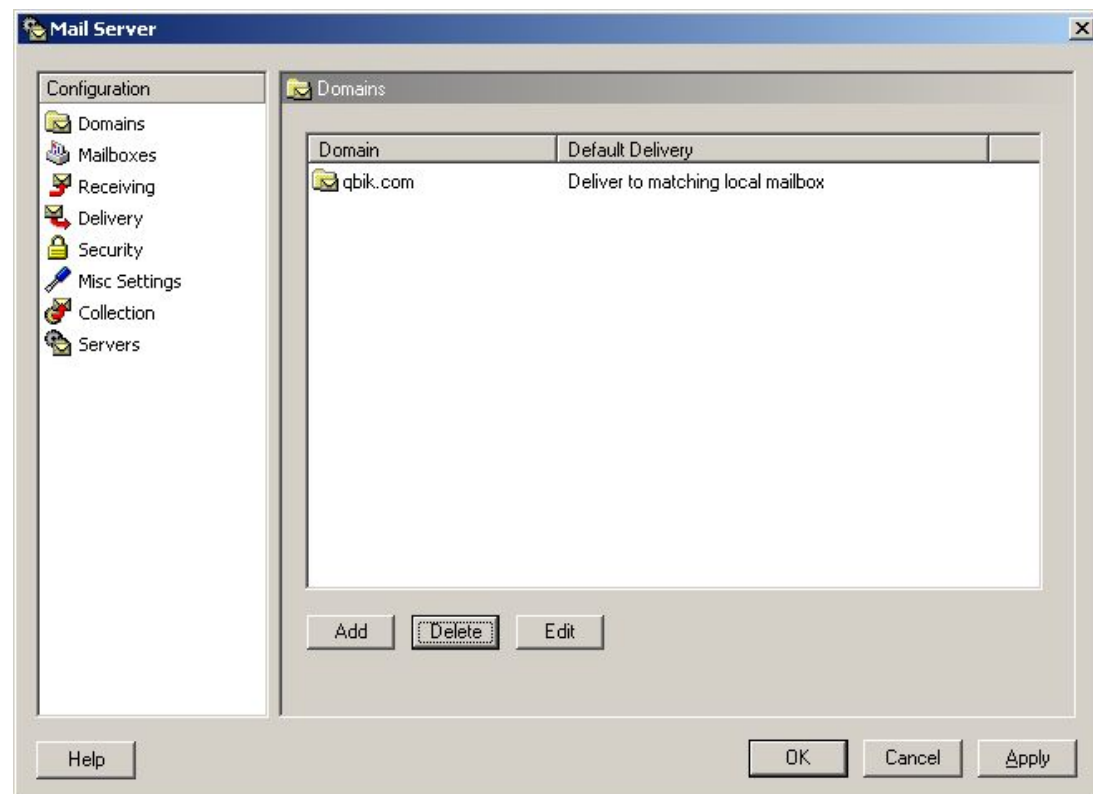
Internet
Computers



In this situation you connect through WinGate (this example presumes that the ENS is installed) to your ISP to collect and send email, and the ISP talks to the other computers on the internet. WinGate can have some involvement in this process, if required. We would recommend that you set your mail clients to send to WinGate, and then point WinGate at the ISP's mail server, as this will provide anti virus scanning. So if Bob is client 1 and sends an email to Frank at Hotmail, then the mail client (say, Outlook) is configured with the ISP's mail server details, and will NAT through WinGate and talk directly with this ISP server (SMTP). Or alternatively, Outlook could send to WinGate's mail server, which will process the mail and send it to the ISP's mail server. This ISP server will, in turn, process the email and send it to Hotmail, where Frank will receive it. When Frank replies, hotmail will talk to the ISP's mail server who will store the message for Bob. Bob can receive the email in two ways. He either set his email program (Outlook) on client 1 to connect to the ISP's mail server (POP3) via WinGate, and download any new messages he has waiting. Or, if the ISP is acting as a 'catchall' for all email addresses at a certain domain (i.e. bob@qbik.com and sales@qbik.com are all stored by the ISP in one mail box) then it would be best to configure a POP Collection from within WinGate mail, which will download all the mail from the 'catchall' mailbox and then parse it out (if configured to do so) across locally held mailboxes on the WinGate machine.

1) WinGate forwards email to the ISP's mail server and uses POP Collection to retrieve email from the ISP's mail server.

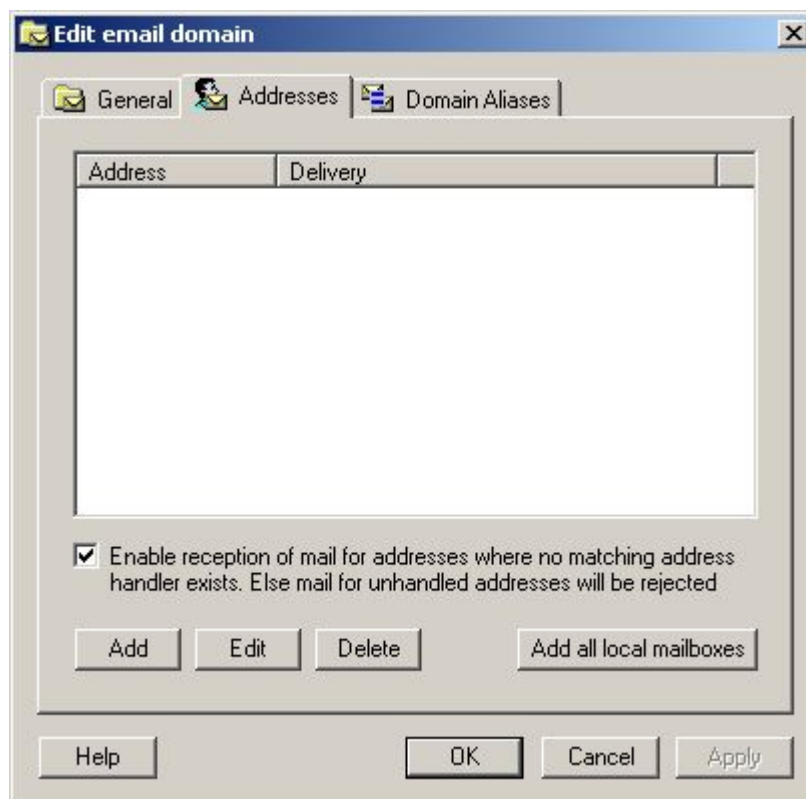
Open the Email properties from the 'System Services' tab in GateKeeper, and under the Domains option, click Add. Enter the name of the domain that is hosted on the ISP's mail server. Here it is qbik.com. Even though WinGate isn't hosting the domain, it still needs to know what your domain is so that it will only allow email from your domain to be sent. (*The Domain you enter needs to have a DNS record located somewhere (either locally by you, or with your service provider)).



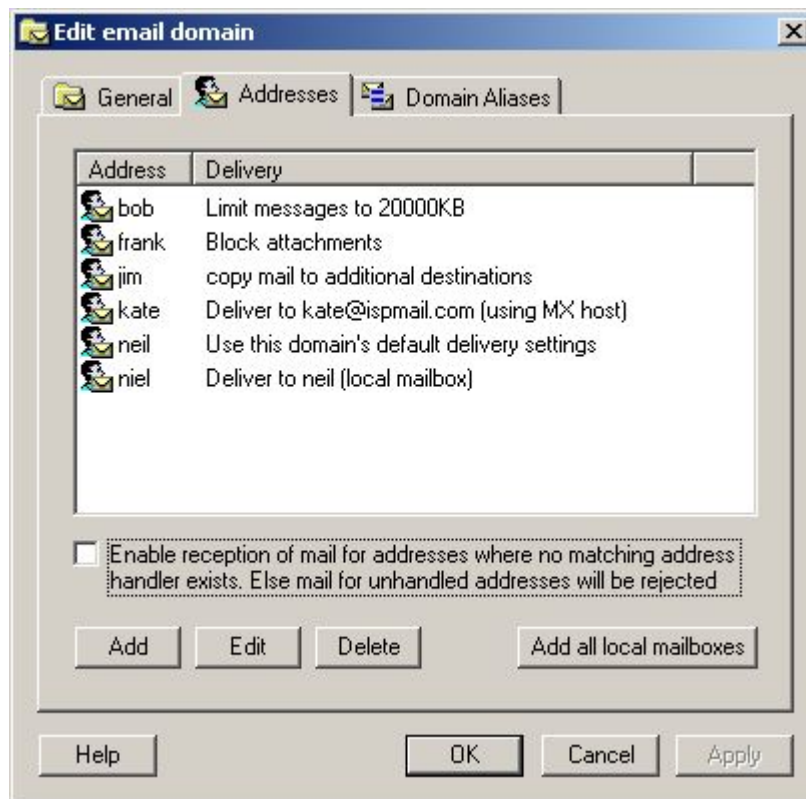
Upon clicking Add, the following screen appears, and it is here that Domain specific properties can be set. The General tab indicates whether this new domain is hosted locally or on another server. In this scenario either could actually be selected, resulting in two slightly different configurations that would give the same result. In most cases 'Mailboxes for this domain are hosted on this server' should be selected, as WinGate will be retrieving email from the ISP's mail server and redistributing it locally, and choosing this option allows for simpler configuration with regard to email handlers. However, it is also possible to specify that 'Mailboxes for this domain are hosted on another server', with remote delivery being performed via MX lookup. This configuration would require specific email handler overrides (see below) for each address/ user to point to a local mailbox, otherwise mail retrieved via POP Collection could end up being looped from WinGate to the ISP's mail server over and over.



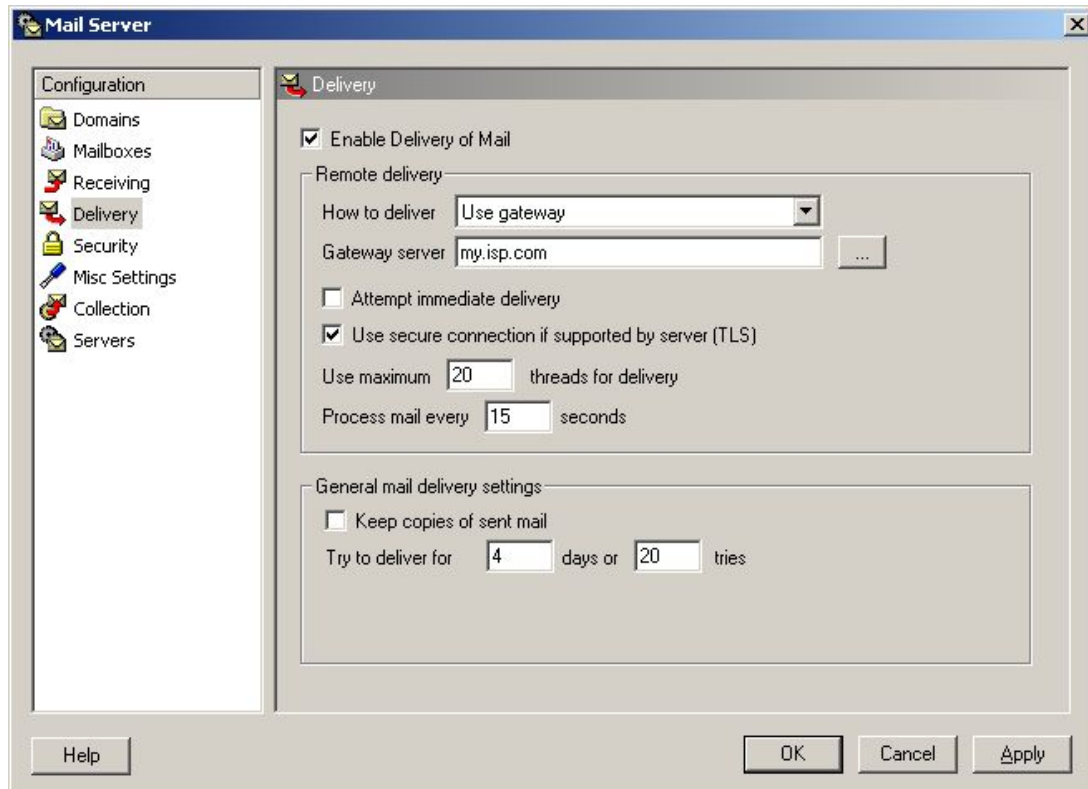
Once this email has been downloaded from the ISP's mail server WinGate then needs to know which users / addresses it should accept mail for. So next, email handlers need to be added to the domain, as it is these two pieces of information (the email handler and the domain) that create the email address. An email handler could be a user name that already exists in WinGate or an 'alias' that points to a user within WinGate. There are several ways WinGate mail can deal with these email handlers. By default the screen will appear blank with the option 'To enable reception of mail for addresses where no matching address handler exists' ticked. This setting effectively means that when WinGate receives an email, it will see that there are no email handlers listed, and so will check the user database (be it NT or the WinGate DB) and if a match is found with a user that is enabled for email then the mail will be accepted and delivered, otherwise it will be rejected. So for example, if the user bob has been created as a user in WinGate, and an email is retrieved for bob@qbik.com (presuming that qbik.com is the domain that is being locally hosted and that POP Collection has been configure as below) , then WinGate will see there is no message handler for bob, but as this option is ticked it will check the user database to see if bob exists there, and as he does, WinGate will accept the email.



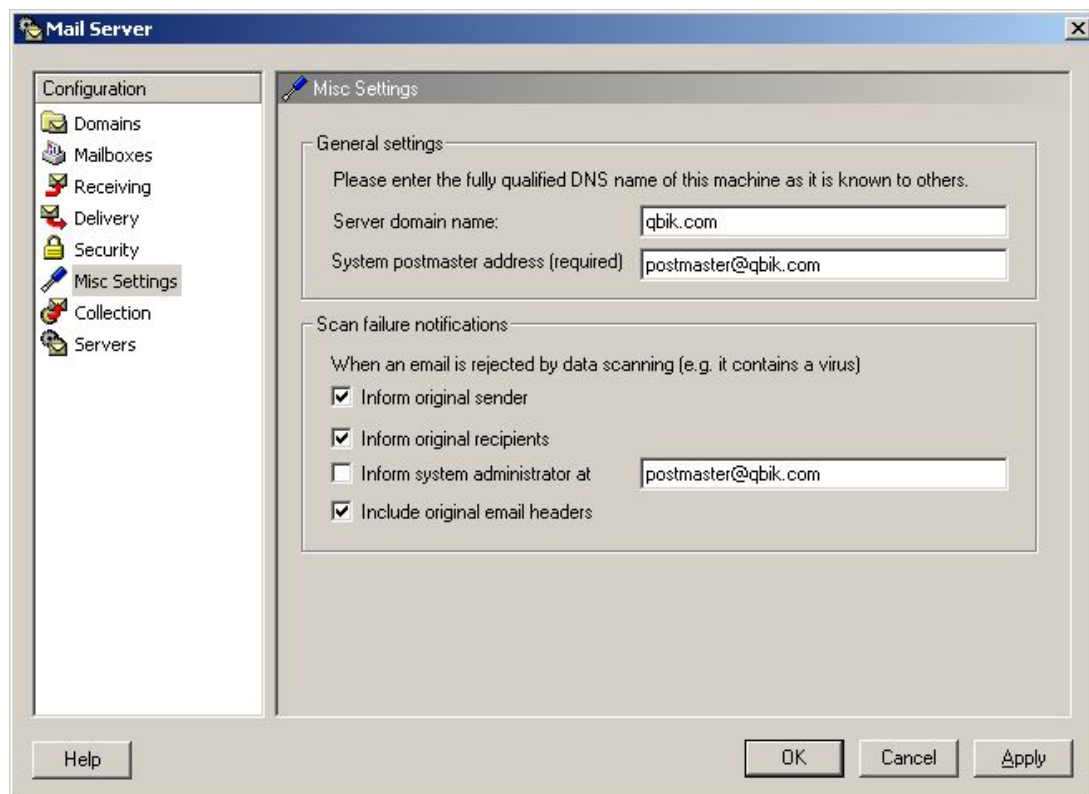
Alternatively, if 'Mailboxes for this domain are hosted on another server' was selected as the domain type above, or only specific users will be allowed to receive email for this domain then the 'Enable reception of mail for addresses where no matching address handler exists' should be UNTicked, and specific email handlers added. This can be done in two ways. If all users need to be added them click 'Add all local mailboxes'; otherwise handlers can be added one at a time until all necessary combinations have been covered.



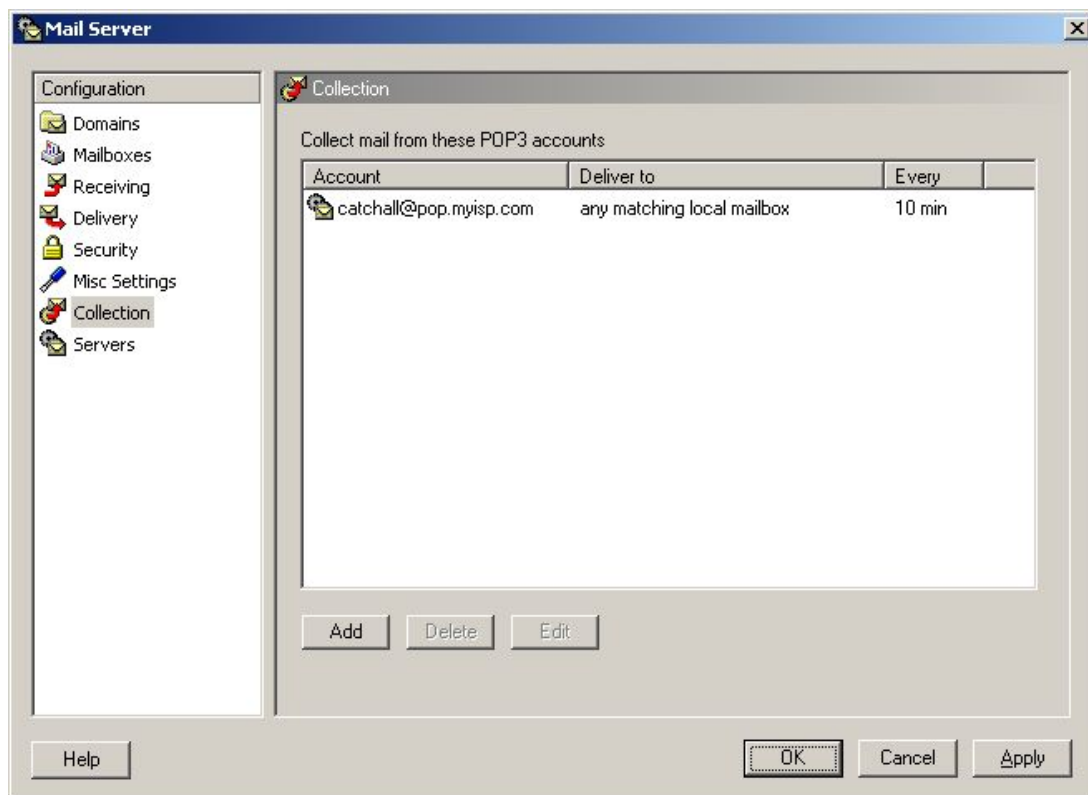
As all outbound email is to be forwarded to the ISP's mail server for delivery on to it's final destination, this needs to set as the default Remote delivery option on the Delivery properties pane. From the 'How to deliver' drop down list choose 'Use Gateway', and enter the ISP mail server's name or IP in the Gateway server option.



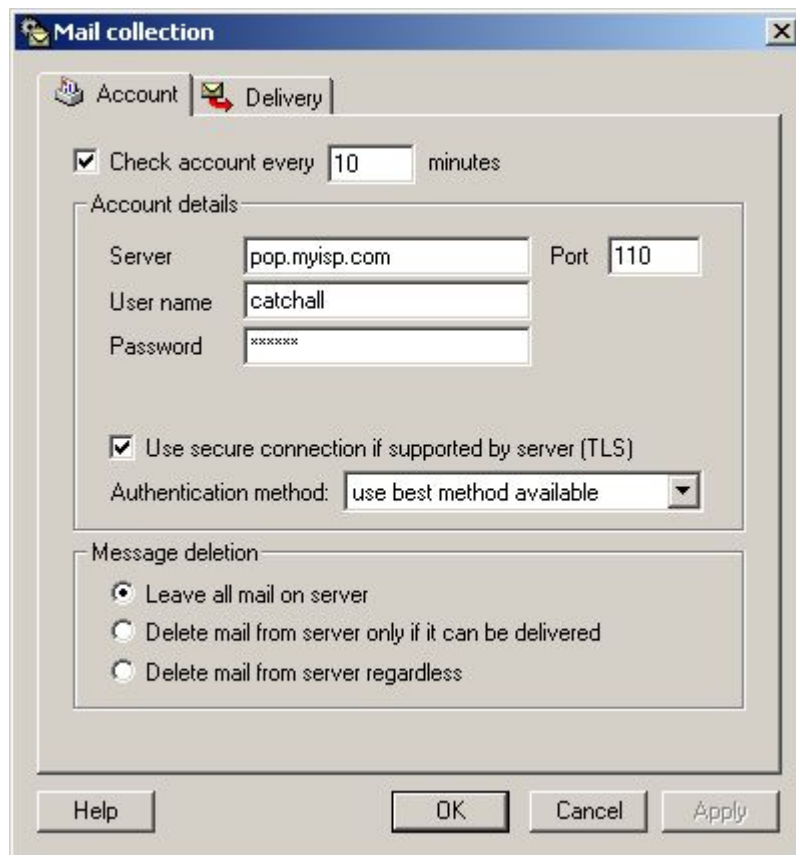
Under the Misc Settings, the Server Domain Name, and the System Postmaster Address MUST be filled out correctly, otherwise mail originating from this server maybe rejected. Although not as important in this scenario as in the previous two, completing this section is still a requirement. The Scan failure notifications configuration is only important if you have Anti Virus for WinGate installed



WinGate is now in a position to send mail out, via the ISP's mail server. However, to be able to receive mail WinGate needs to retrieve it from this remote ISP server. This is done with POP Collection, which is configured under the Collection pane.



To create a new POP Collection click Add. Under the Account tab, the basic details of the collection are specified, such as the ISP mail server hosting the mail that is to be retrieved, the username and password of the mailbox that the collection will connect to, and any special requirements that the ISP may have for this connection, such as a particular authentication method. Also on the Account tab, the Message deletion options can be set, and the interval at which this collection should check the remote server for new mail.

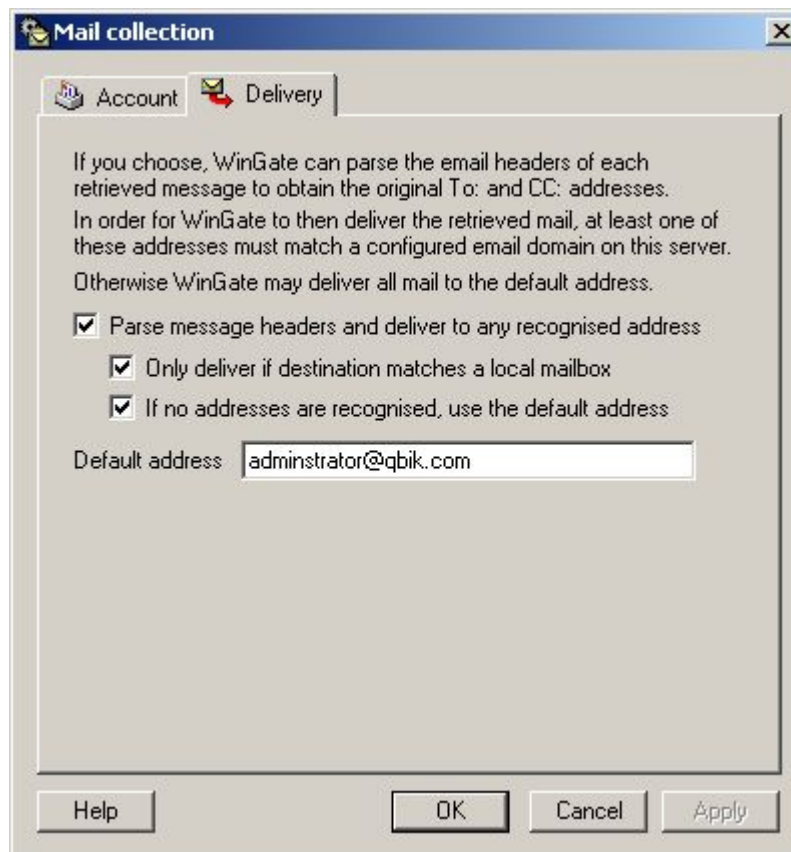


The image shows a 'Mail collection' dialog box with two tabs: 'Account' and 'Delivery'. The 'Account' tab is selected. It contains the following fields and options:

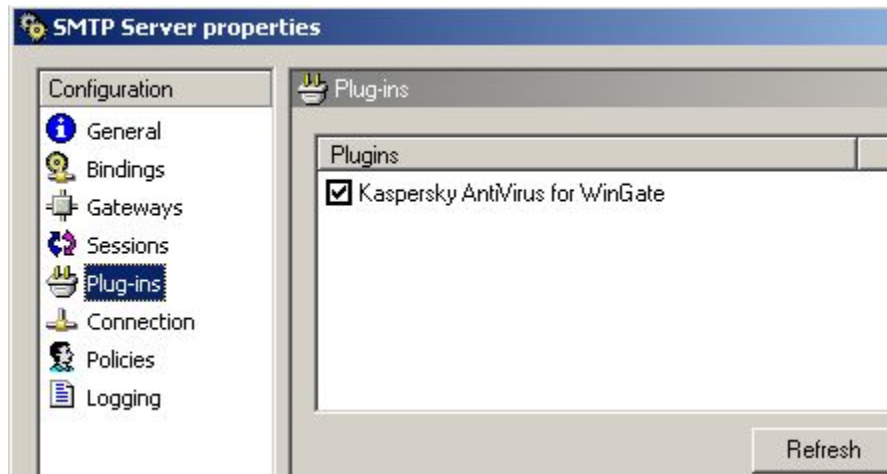
- ☒ Check account every minutes
- Account details**
 - Server: Port:
 - User name:
 - Password:
- ☒ Use secure connection if supported by server (TLS)
- Authentication method:
- Message deletion**
 - ☒ Leave all mail on server
 - ☐ Delete mail from server only if it can be delivered
 - ☐ Delete mail from server regardless

At the bottom are buttons for 'Help', 'OK', 'Cancel', and 'Apply'.

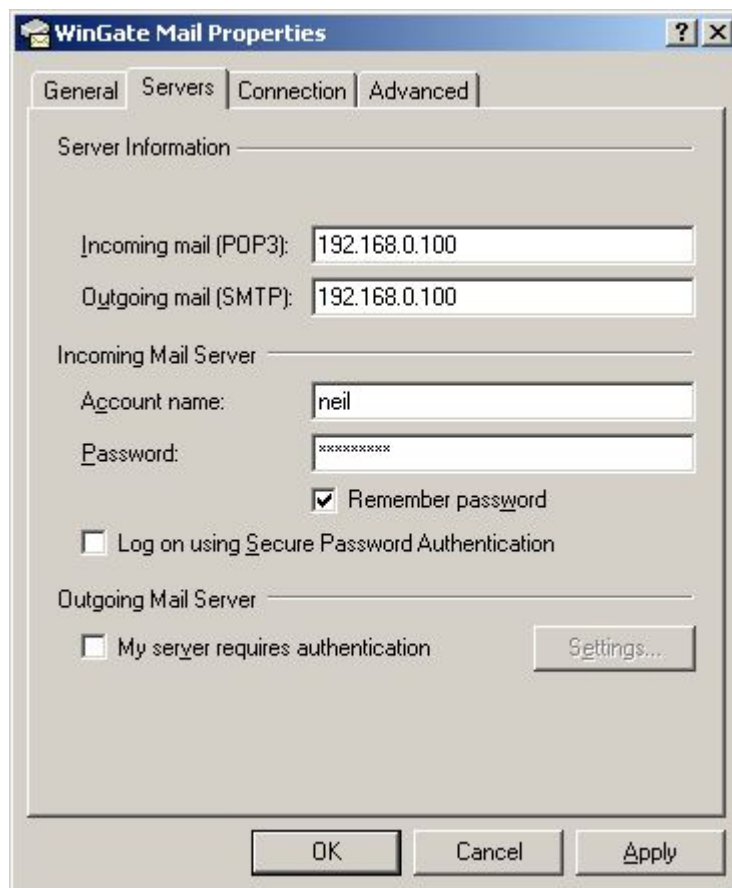
The Delivery tab specifies how the mail should be processed for delivery once it has been downloaded. The default configuration for a new POP Collection is to parse the newly downloaded message headers and to deliver to any To: or CC: addresses it recognises. It does this by matching these fields to email handlers and the domain, that have been configured previously in WinGate mail, hence the importance of these two earlier steps; otherwise legitimate email could accidentally be discarded due to mis-configuration. POP Collection can also be set to only deliver if the address parsed from the downloaded email matches a local mailbox, or to deliver all mail with un-recognised addresses to a default / catchall address, in this case administrator@qbik.com.



As WinGate won't be receiving any email in this scenario, the Bindings do not need to be altered from the defaults. This is because, to send email out, WinGate doesn't require to be bound to an external interface, and POP Collection replaces the need to receive mail. Finally, if you have any WinGate Anti-Virus product installed, check to make sure the Anti-Virus scanning is enabled in the SMTP Server properties, as mail retrieved via POP Collection, will be scanned before being delivered, as well as all outbound mail.



WinGate is now configured to virus scan and then send mail on to the ISP's mail server for further delivery, and also to retrieve remotely hosted email via POP Collection. The next step is to configure the email clients, such as Outlook, Outlook Express, or The Bat etc. These Client machines then need to have their SMTP and Pop3 settings pointed to the WinGate machine's IP address. This example shows the entries that would be made in Outlook Express if the WinGate server's IP was 192.168.0.100.



The image shows a screenshot of the 'WinGate Mail Properties' dialog box. The 'General' tab is selected. Under 'Server Information', the 'Incoming mail (POP3):' and 'Outgoing mail (SMTP):' fields both contain the IP address '192.168.0.100'. Under 'Incoming Mail Server', the 'Account name:' field contains 'neil' and the 'Password:' field contains a series of asterisks. The 'Remember password' checkbox is checked, and the 'Log on using Secure Password Authentication' checkbox is unchecked. Under 'Outgoing Mail Server', the 'My server requires authentication' checkbox is unchecked. There is a 'Settings...' button next to the 'My server requires authentication' checkbox. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

WinGate Mail Properties

General Servers Connection Advanced

Server Information

Incoming mail (POP3): 192.168.0.100

Outgoing mail (SMTP): 192.168.0.100

Incoming Mail Server

Account name: neil

Password: xxxxxxxx

☒ Remember password

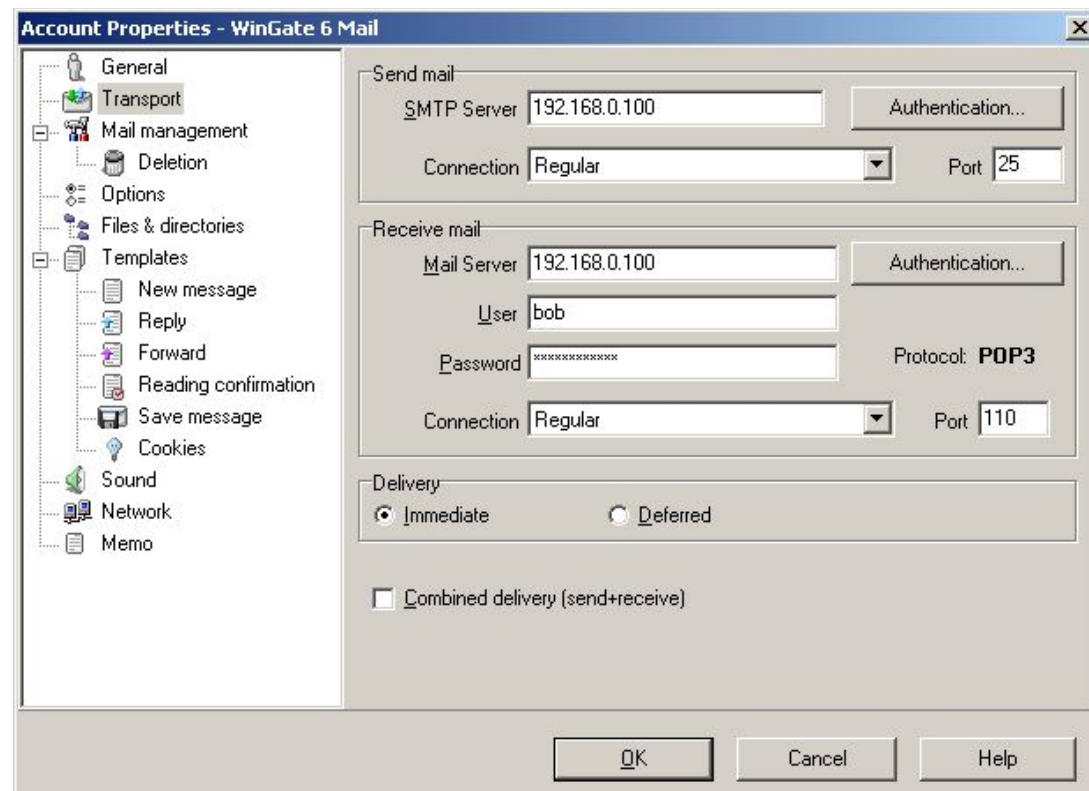
☐ Log on using Secure Password Authentication

Outgoing Mail Server

☐ My server requires authentication Settings...

OK Cancel Apply

This example shows the entries that would be made in The Bat if the WinGate server's IP was 192.168.0.100.

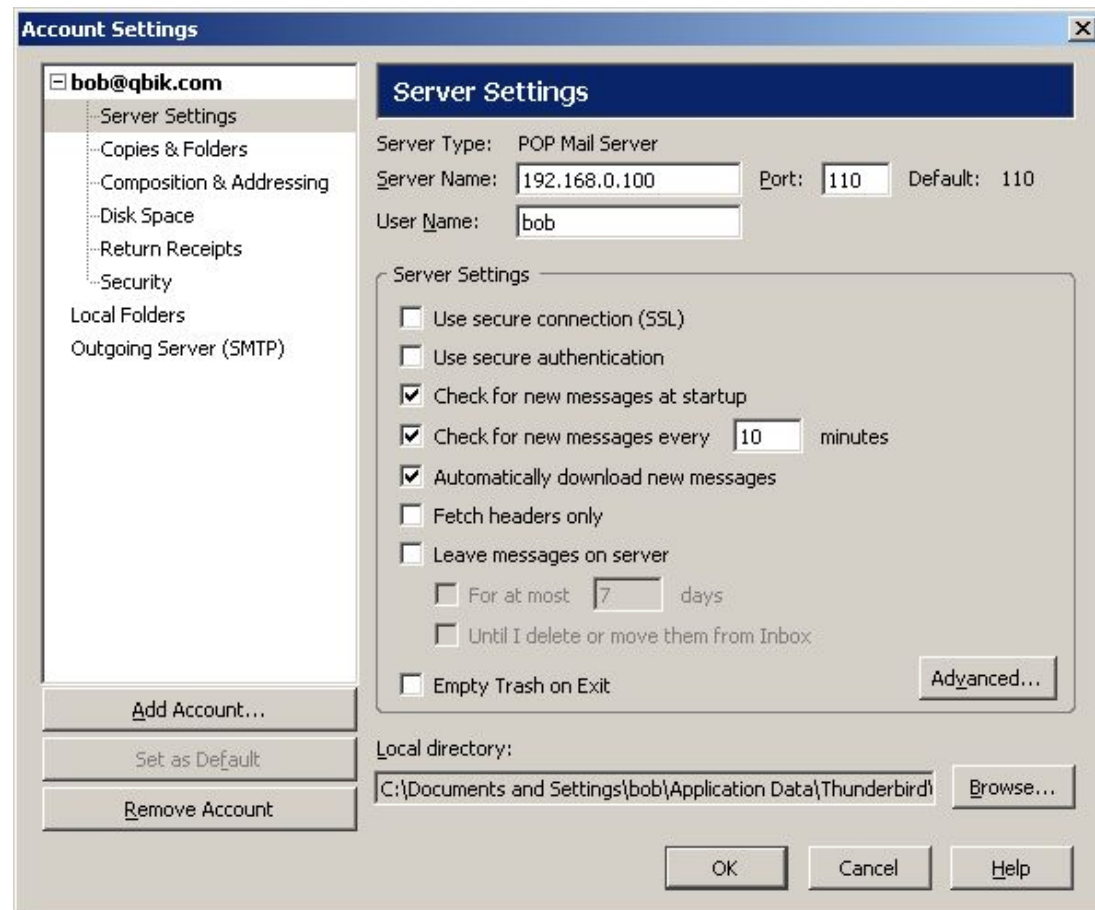


This example shows how Outlook XP would be configured if the WinGate server's IP was 192.168.0.100

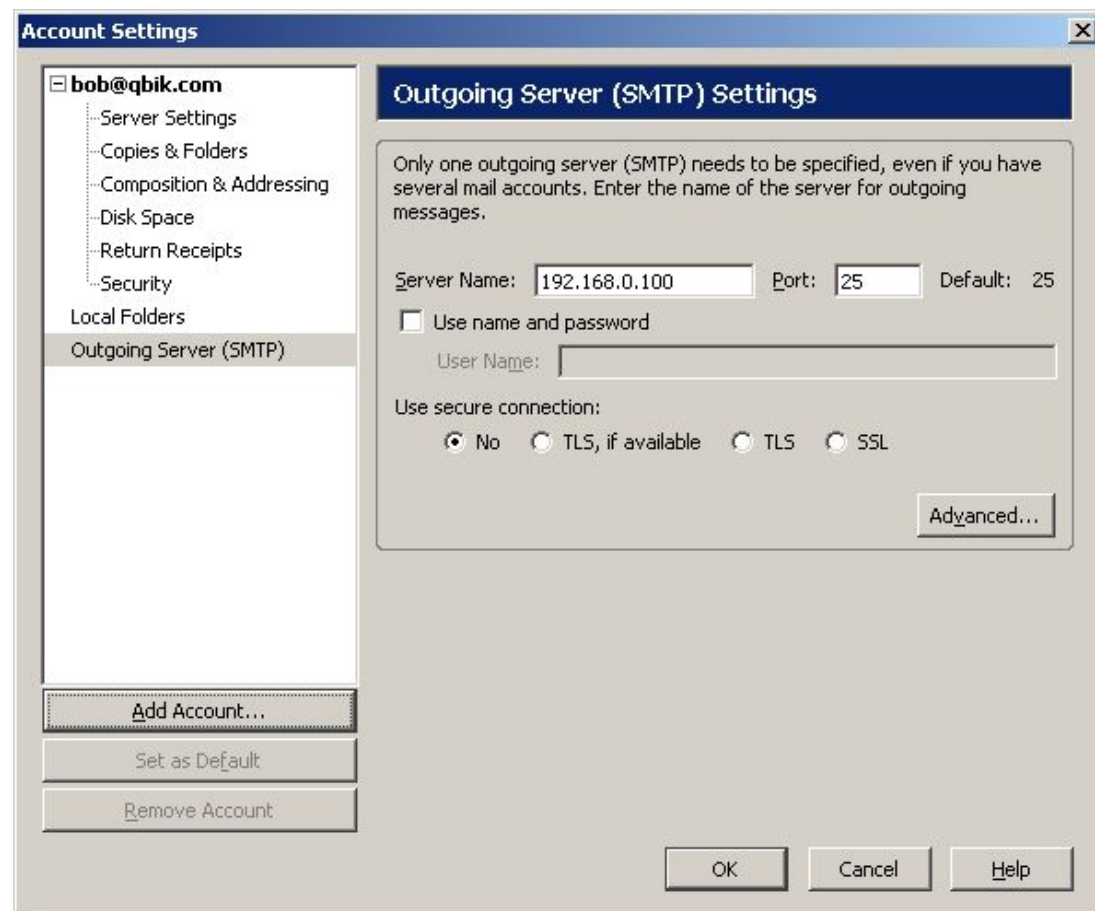


This example shows how Thunderbird would be configured if the WinGate server's IP was 192.168.0.100

Firstly POP3:

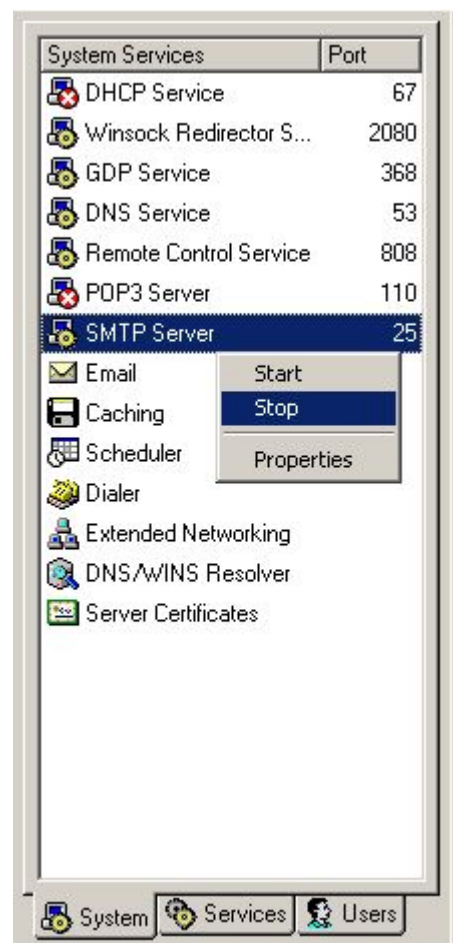


Then SMTP:

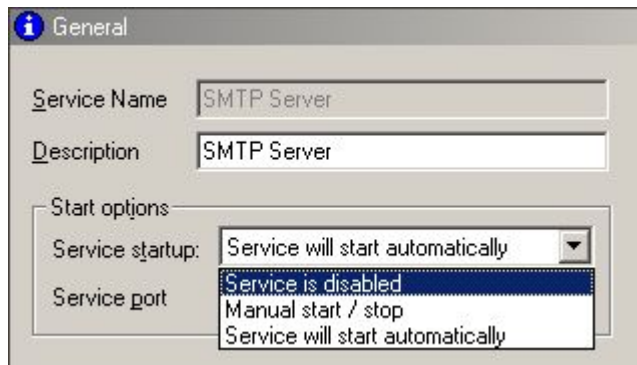


2) If it would be preferable to have the email clients on the LAN simply 'pass through' WinGate to connect to the ISP's mail server to send and receive email, then WinGate needs to be additionally configured as follows (This description presumes the ENS is installed):

As none of WinGate's specific mail functions will be used, these will need to be switched off, to stop them interfering when mail is trying to 'pass through'. To do this, right click on both the POP3 and SMTP Servers in the System Services tab and select Stop.



Each service then needs to be modified so that it will not restart again if the WinGate engine is restarted. To do this, bring up the properties window for both the SMTP and POP server (one at a time) by right clicking on the service. Then from the Service Start-up drop down list on the General pane, select Service is disabled.



The email clients, such as Outlook, Outlook Express, or The Bat etc, on LAN PC's need to be configured to point at the ISP's mail server and not WinGate. The client PC's will also need a way of connecting to the internet, such as NAT or the WinGate Internet Client. This example shows the entries that would be made in Outlook Express.

Mail hosted on myisp.com Properties

General Servers Connection Advanced

Server Information

Incoming mail (POP3): pop.myisp.com

Outgoing mail (SMTP): smtp.myisp.com

Incoming Mail Server

Account name: bob

Password: xxxxxxxx

☒ Remember password

☐ Log on using Secure Password Authentication

Outgoing Mail Server

☐ My server requires authentication

Settings...

OK Cancel Apply

And this example shows the entries that would be made in The Bat.

Account Properties - WinGate 6 Mail

General

Transport

Send mail

SMTP Server: my.isp.com Authentication...

Connection: Regular Port: 25

Receive mail

Mail Server: my.isp.com Authentication...

User: bob

Password: xxxxxxxxxxxx Protocol: POP3

Connection: Regular Port: 110

Delivery

☒ Immediate ☐ Deferred

☐ Combined delivery (send+receive)

OK Cancel Help

And this example shows the entries that would be made in Outlook XP.

E-mail Accounts

Internet E-mail Settings (POP3)

Each of these settings are required to get your e-mail account working.

User Information

Your Name: bob

E-mail Address: bob@qbik.com

Server Information

Incoming mail server (POP3): my.isp.com

Outgoing mail server (SMTP): my.isp.com

Logon Information

User Name: bob

Password: xxxxxxxxxx

☒ Remember password

☐ Log on using Secure Password Authentication (SPA)

Test Settings

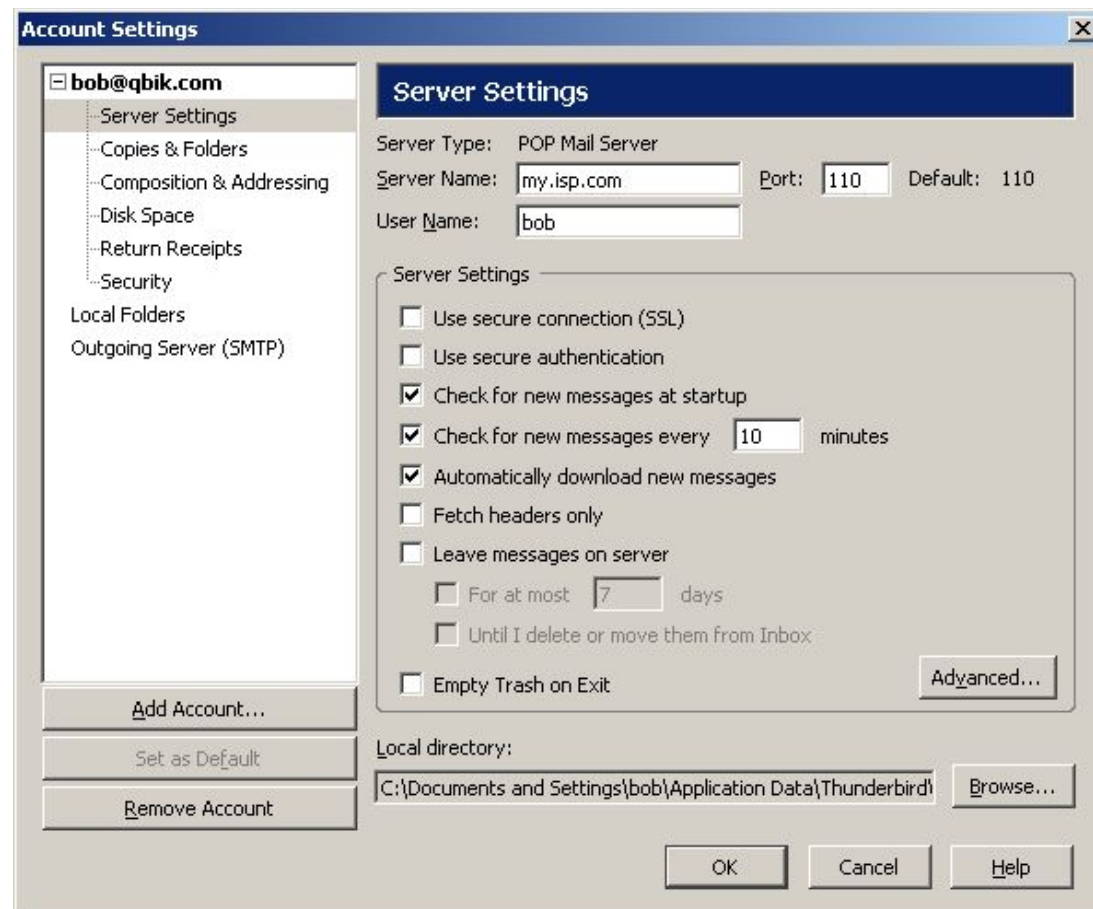
After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

Test Account Settings ...

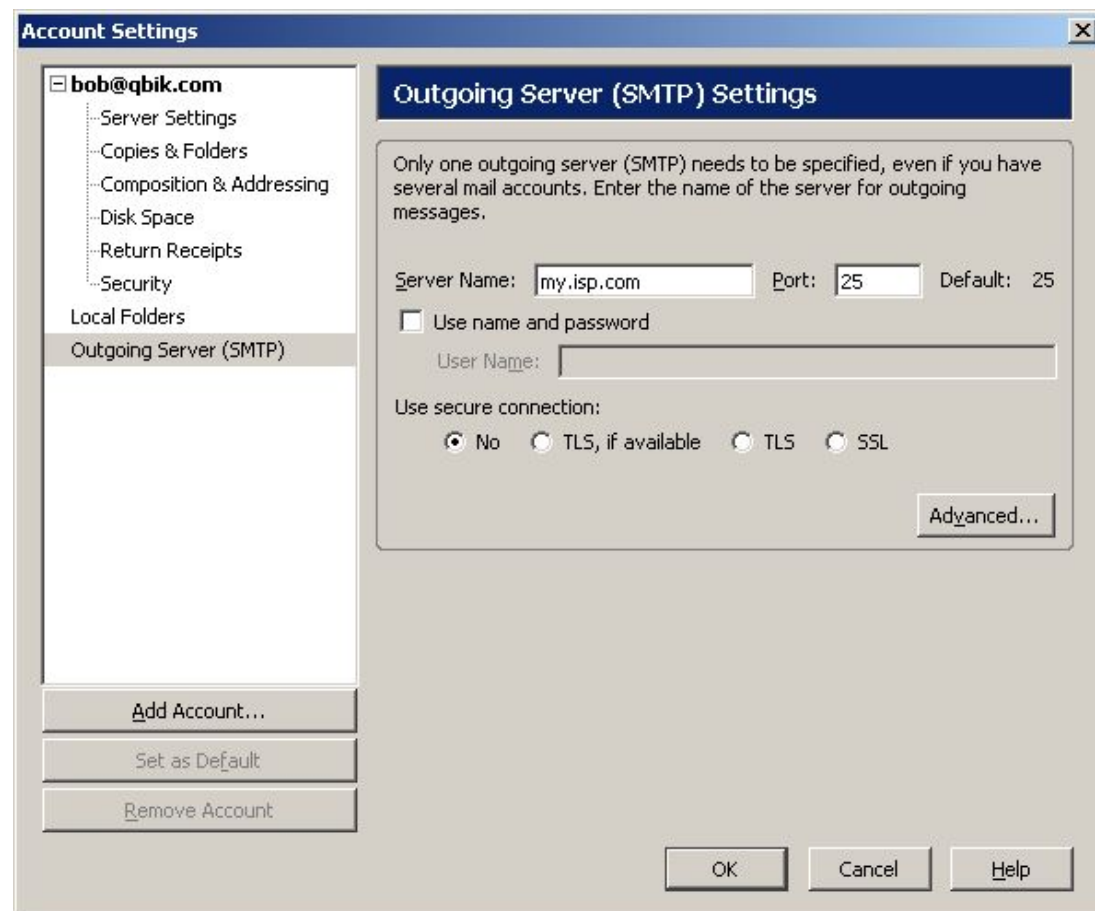
More Settings ...

< Back Next > Cancel

And this example shows the entries that would be made in Thunderbird. Firstly POP3:



Then SMTP:

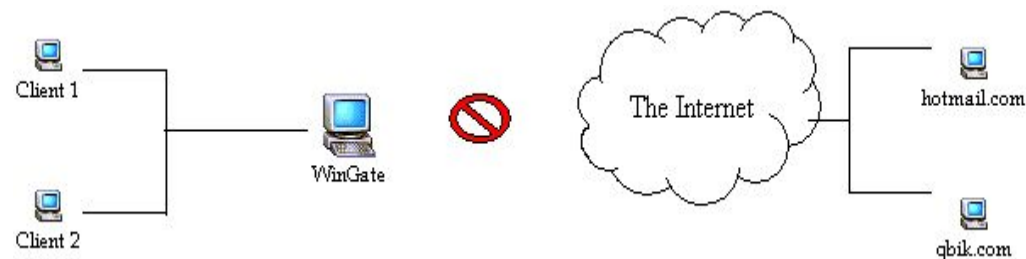


Scenario 4:

Using WinGate for a non-internet, LAN only Mail Server.

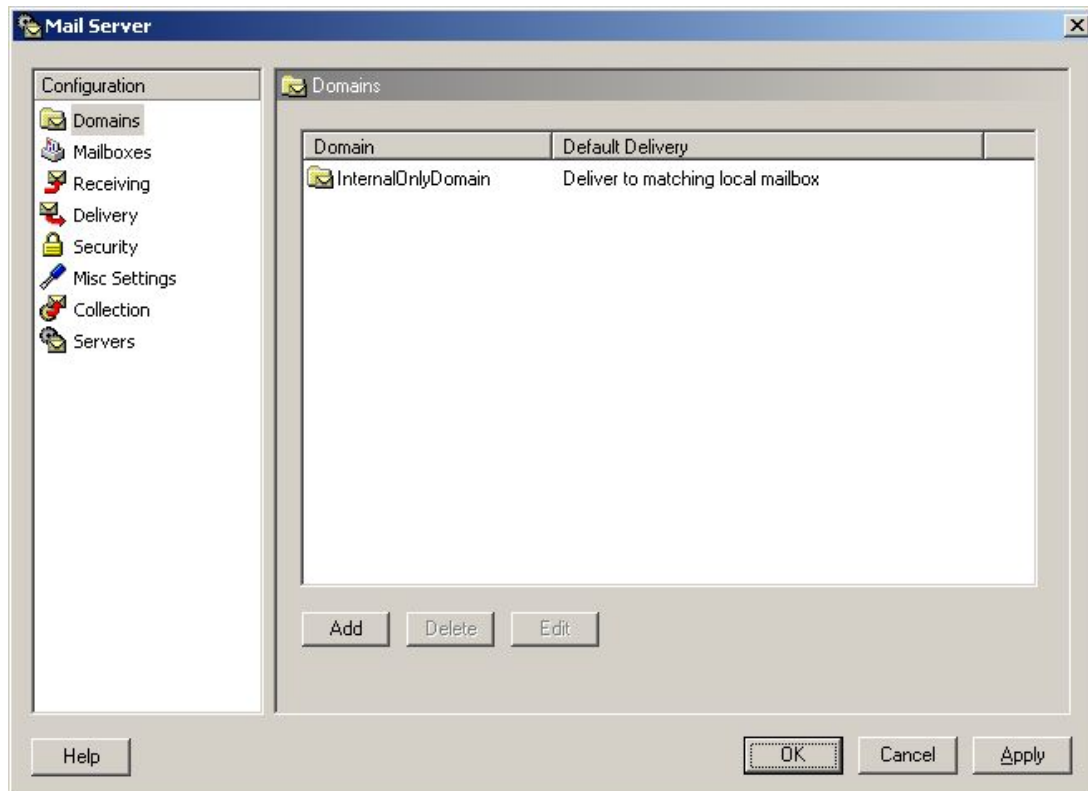
Computers on your LAN
(Local Area Network)

Internet Computers

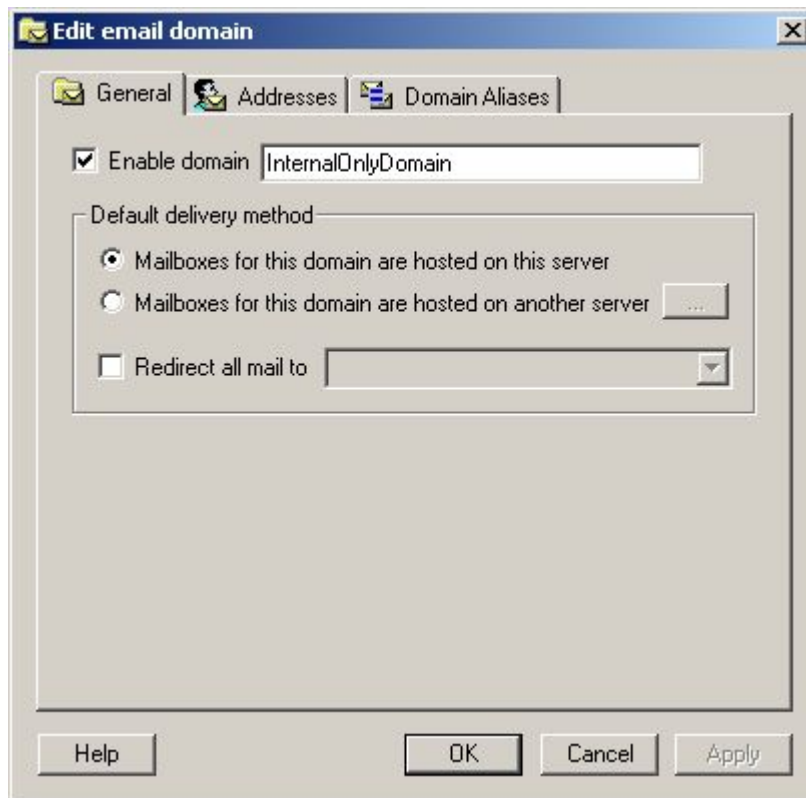


In this scenario, WinGate mail is run purely as an internal mail server. That is, no one from the LAN can send mail out to the internet, and no one outside of the LAN can send emails in. There are many possible benefits of such a situation. Firstly it's very secure, as no virus's or spam can get in, and anything trying to get out will fail. It is also a useful way for small companies who don't own, or require, a domain to communicate between each other. There are a number of ways this scenario could be set up, this description will detail the most secure way.

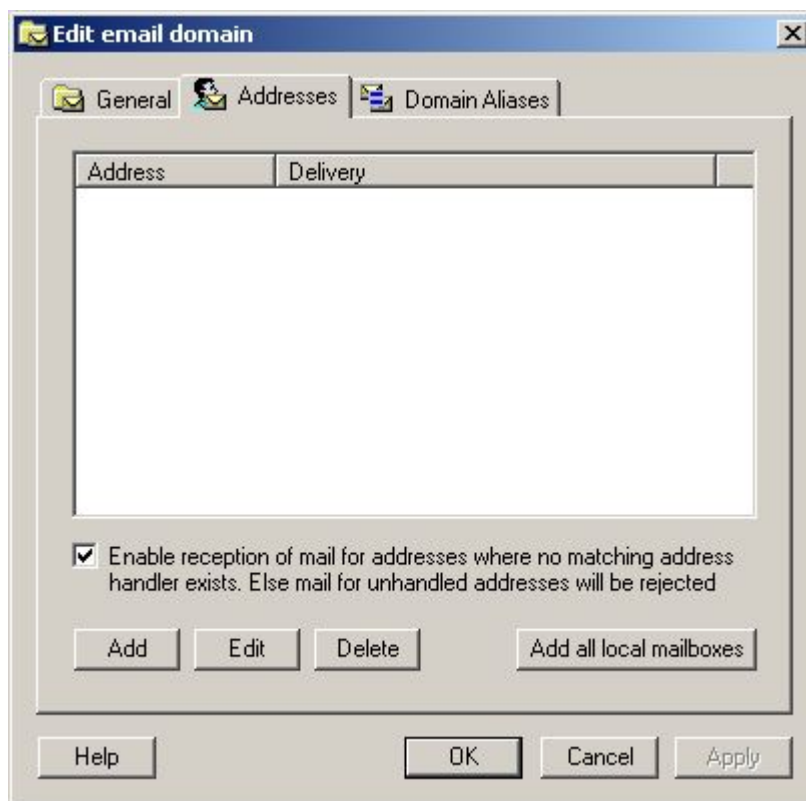
Open the Email properties from the 'System Services' tab in GateKeeper, and under the Domains option, click Add. As this is for a domain that won't come in to contact with the internet, it can be anything, and doesn't require a DNS record. It is recommended, for this scenario, that a domain is chosen that couldn't actually exist in the 'real' world of the internet; i.e. nothing that ends in .com etc.



Upon clicking Add the following screen appears, and it is here that Domain specific properties can be set. The General tab indicates whether this new domain is hosted locally or on another server. As this set-up is purely for internal use, the option 'Mailboxes for this domain are hosted on this server' should be selected.



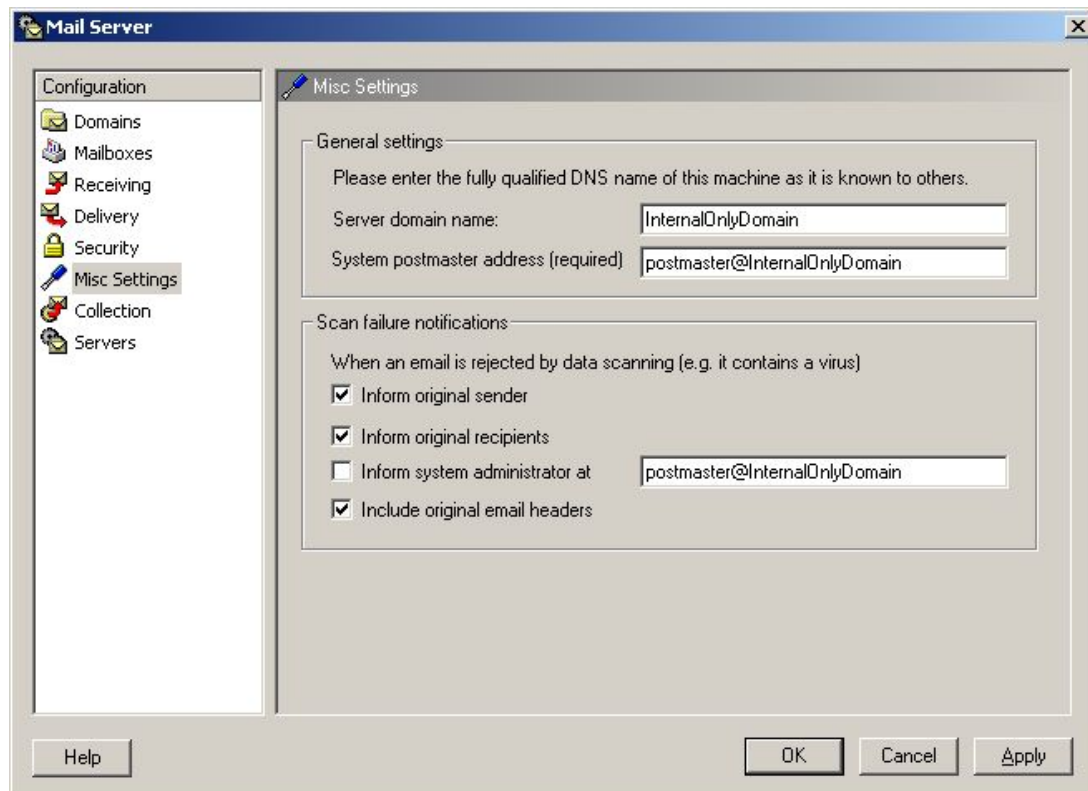
Next email handlers need to be added and there are several ways that WinGate mail can deal with them (for more detailed information on Email Handlers see the Features section above). By default the screen will appear blank with the option 'To enable reception of mail for addresses where no matching address handler exists' ticked. This setting effectively means that when WinGate receives an email, it will see that there are no email handlers listed, and so will check the user database (be it NT or the WinGate DB) and if a match is found with a user that is enabled for email then the mail will be accepted and delivered, otherwise it will be rejected. So for example, if the user bob has been created as a user in WinGate, and an email is sent to bob@InternalOnlyDomain, then WinGate will see there is no message handler for bob, but as this option is ticked it will check the user database to see if bob exists there, and as he does, WinGate will deliver the mail. This is probably the best option for this scenario, as it requires the least amount of set-up, and the need for overrides to restrict a user's mailbox is limited



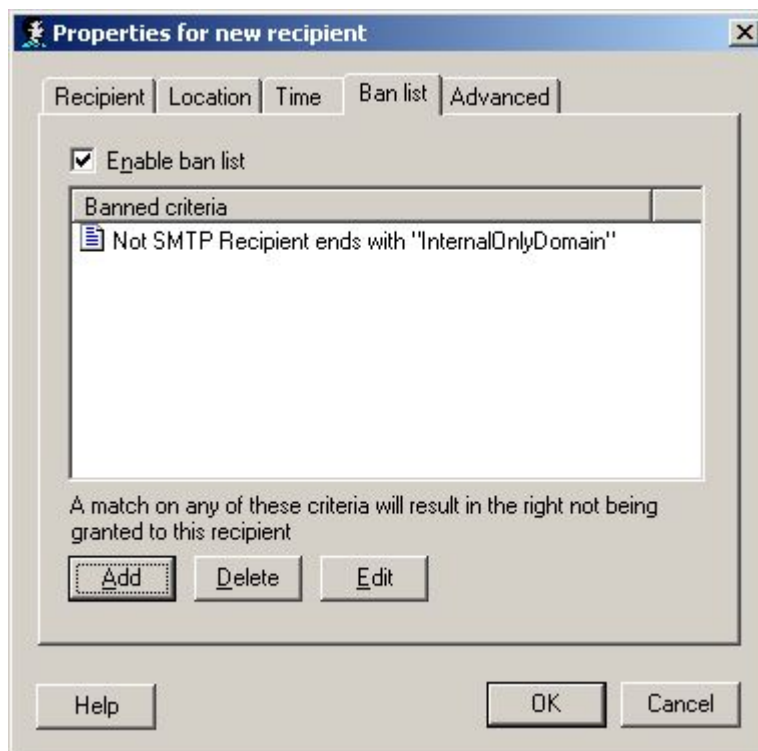
However, if email handler overrides are required, so that only specific users will be allowed to receive email on this domain (or others have restrictions placed upon them), then the 'Enable reception of mail for addresses where no matching address handler exists' should be UNTicked, and specific email handlers added. This can be done in two ways. If all users need to be added them click 'Add all local mailboxes'; otherwise handlers can be added one at a time until all necessary combinations have been covered.



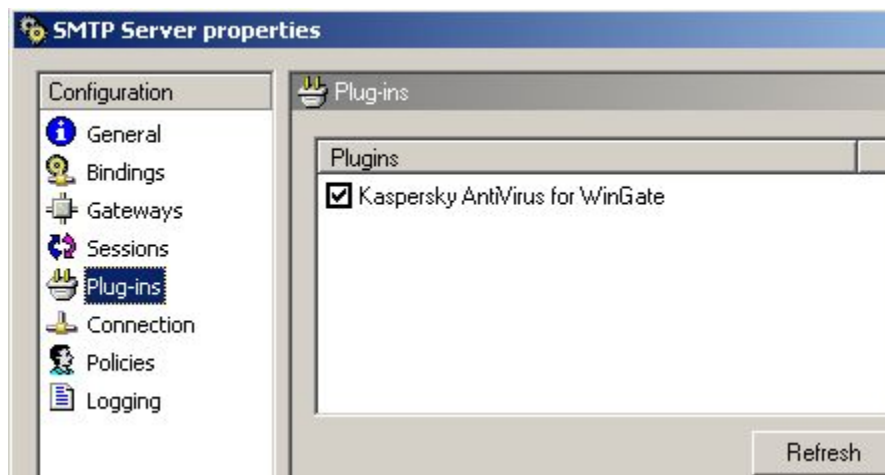
Most of the other options available, in the Mail Server properties, don't affect this scenario, but can be tweaked if desired. The Misc options still need to be filled out however, although the information entered is less important here than in other scenarios, as it will not be communicating with other Mail Servers.



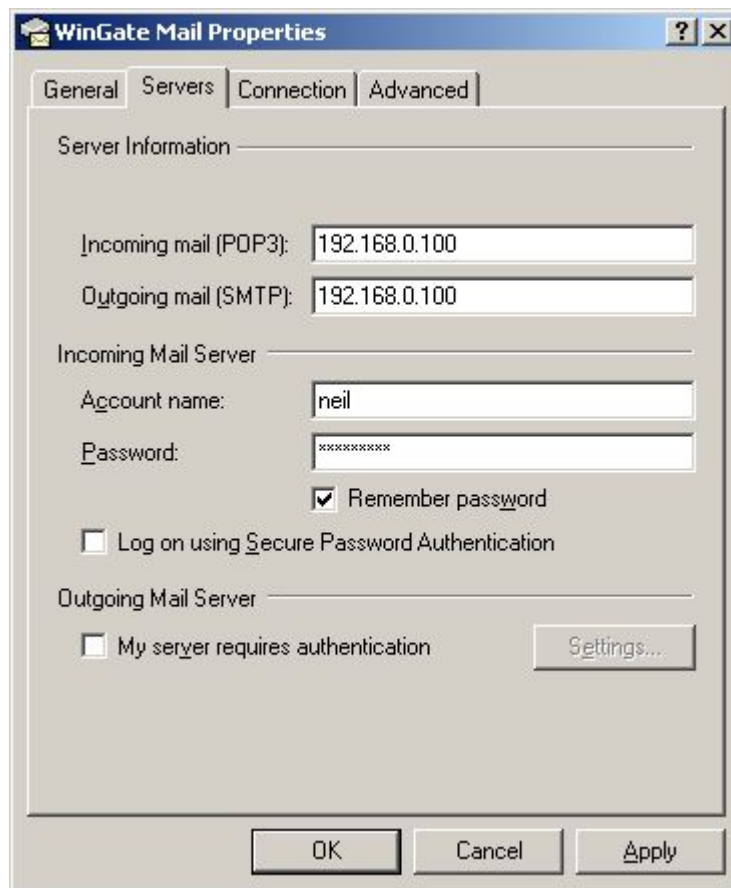
Now WinGate is set-up to send and receive email for a LAN only. As this domain will not be receiving email from the outside (internet) world, the SMTP bindings defaults can be left alone, as they are set to only allow connections from trusted / internal adapters. However to prevent users on the LAN sending to users on the internet, an SMTP policy needs to be set. This is done under the policies pane in SMTP server properties. Click Add, to create a new policy, and go to the Ban List tab. Enable the Ban List, and click Add again, and create a criterion of 'This criterion is NOT met if – SMTP Recipient –ends with – InternalOnlyDomain' (assuming InternalOnlyDomain is the name that has been chosen for the domain).



Finally, if you have any WinGate Anti-Virus product installed, check to make sure the Anti-Virus scanning is enabled in the SMTP Server properties, although by virtue of having restricted access to the mail server in this scenario, this step is for the extra cautious.



WinGate is now configured to act as the internal only 'protected' mail server on the network. The next step is to configure the email clients, such as Outlook, Outlook Express, or The Bat etc. These Client machines then need to have their SMTP and Pop3 settings pointed to the WinGate machine's IP address. This example shows the entries that would be made in Outlook Express if the WinGate server's IP was 192.168.0.100.



The image shows a screenshot of the 'WinGate Mail Properties' dialog box. The 'General' tab is selected. Under 'Server Information', the 'Incoming mail (POP3):' and 'Outgoing mail (SMTP):' fields both contain the IP address '192.168.0.100'. Under 'Incoming Mail Server', the 'Account name:' field contains 'neil' and the 'Password:' field contains 'xxxxxxx'. The 'Remember password' checkbox is checked, and the 'Log on using Secure Password Authentication' checkbox is unchecked. Under 'Outgoing Mail Server', the 'My server requires authentication' checkbox is unchecked. There is a 'Settings...' button next to the 'My server requires authentication' checkbox. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

WinGate Mail Properties

General Servers Connection Advanced

Server Information

Incoming mail (POP3): 192.168.0.100

Outgoing mail (SMTP): 192.168.0.100

Incoming Mail Server

Account name: neil

Password: xxxxxxx

☒ Remember password

☐ Log on using Secure Password Authentication

Outgoing Mail Server

☐ My server requires authentication Settings...

OK Cancel Apply

This example shows the entries that would be made in The Bat if the WinGate server's IP was 192.168.0.100.

Account Properties - WinGate 6 Mail

Send mail

SMTP Server: 192.168.0.100 Authentication...

Connection: Regular Port: 25

Receive mail

Mail Server: 192.168.0.100 Authentication...

User: bob Password: Password masked Protocol: POP3

Connection: Regular Port: 110

Delivery

☒ Immediate ☐ Deferred

☐ Combined delivery (send+receive)

OK Cancel Help

This example shows the entries that would be made in Outlook XP if the WinGate server's IP was 192.168.0.100.

E-mail Accounts

Internet E-mail Settings (POP3)

Each of these settings are required to get your e-mail account working.

User Information

Your Name: bob

E-mail Address: bob@qbik.com

Server Information

Incoming mail server (POP3): 192.168.0.100

Outgoing mail server (SMTP): 192.168.0.100

Logon Information

User Name: bob

Password: Password masked

☒ Remember password

☐ Log on using Secure Password Authentication (SPA)

Test Settings

After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

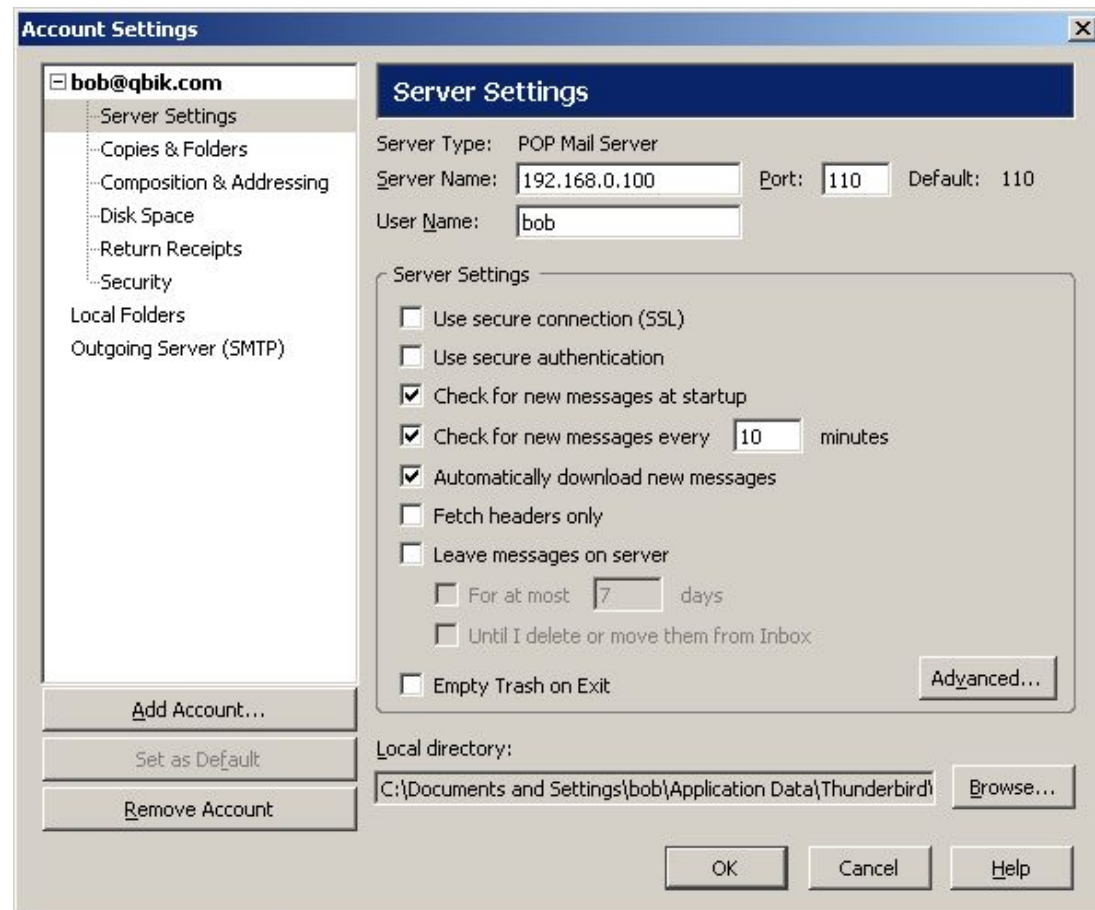
Test Account Settings ...

More Settings ...

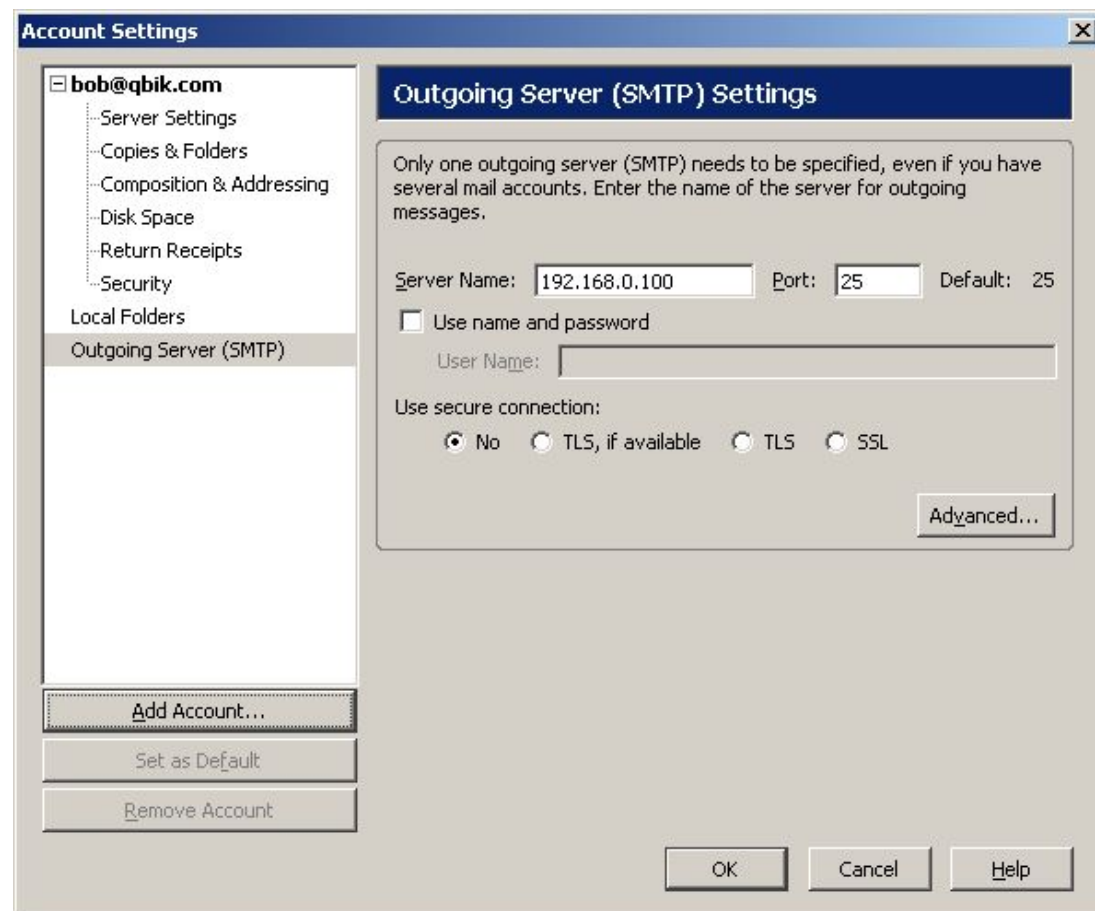
< Back Next > Cancel

This example shows the entries that would be made in Thunderbird if the WinGate server's IP was 192.168.0.100.

Firstly POP3:



Then SMTP:

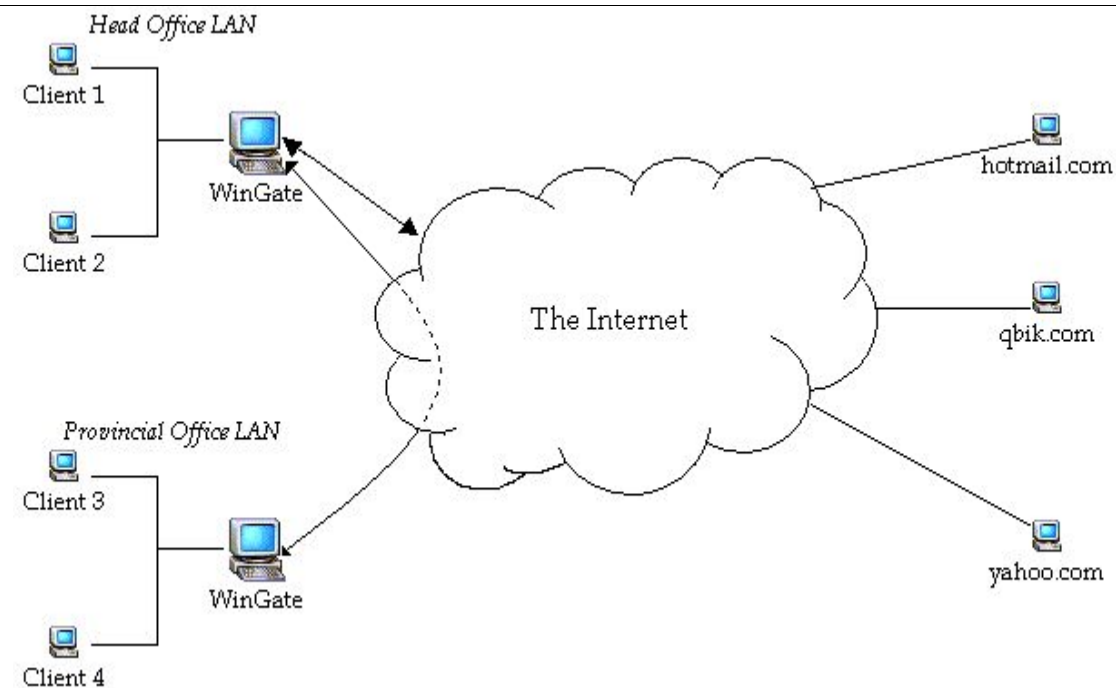


Scenario 5

Using WinGate mail for Multi office / single domain

Computers on your LAN
(Local Area Network)

Internet Computers

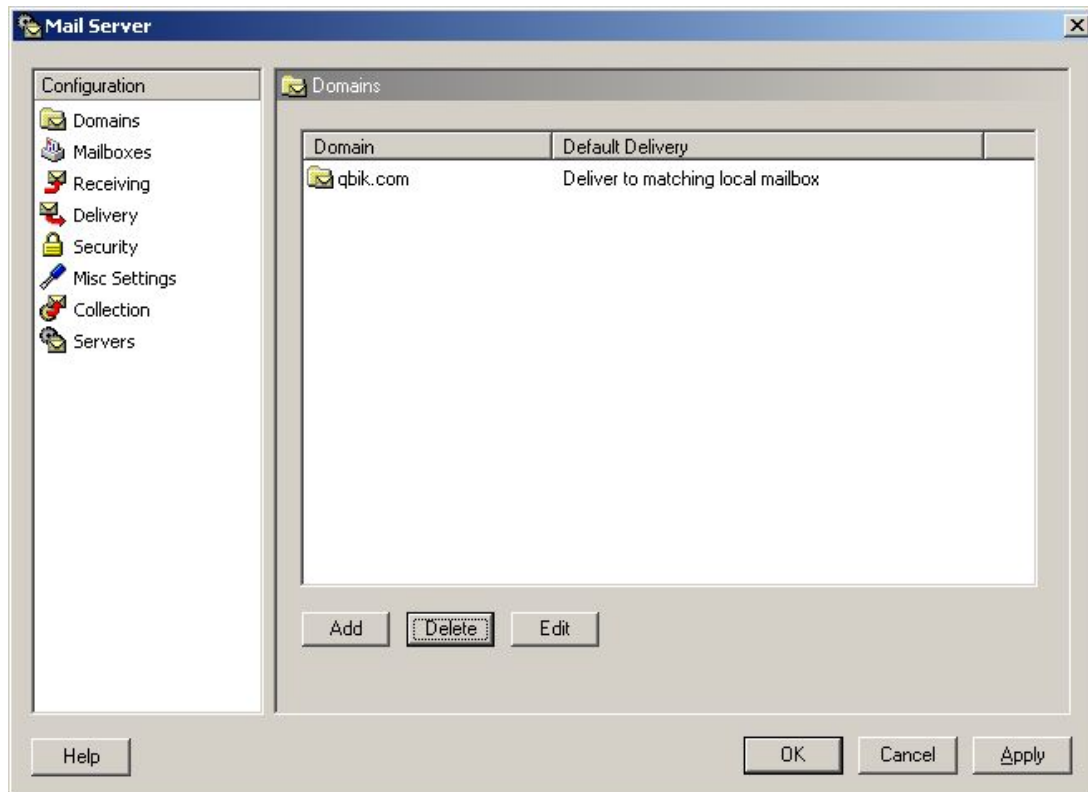


In this situation, the head office is the main mail server for the company, with the DNS record for the domain pointing to the Head Offices IP. But the company has multiple offices around the country. For these other offices to get their mail, the Head Office mail server either has to push (i.e. forward on) the mail to these other offices, or these remote offices have to connect to Head Office and retrieve the mail themselves via a mechanism such as POP Collection (explained above). Similarly, if bob is using Client 4 in the Provincial Office, and wants to send an email to frank@hotmail.com then the Provincial Office can either be set up to deliver to Hotmail directly, or if the company has a policy (for monitoring purposes etc) whereby all outbound mail should go through the Head Office server, then the Provincial Office mail server can be configured to forward all email on to Head Office for processing and delivery. This section will detail how WinGate needs to be configured for the scenario of the Provincial Office forwarding email to the Head Office for delivery, and the Head Office pushes received internet email back to the Provincial Office.

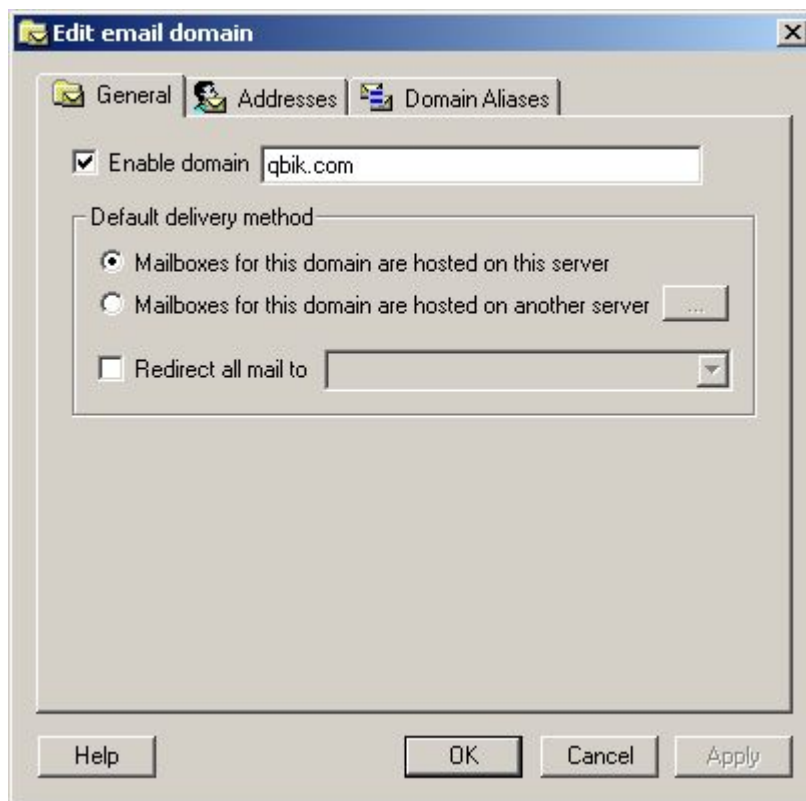
Head Office WinGate Mail Configuration

The Head Office set-up is very similar to a standard WinGate Mail set-up (see above)

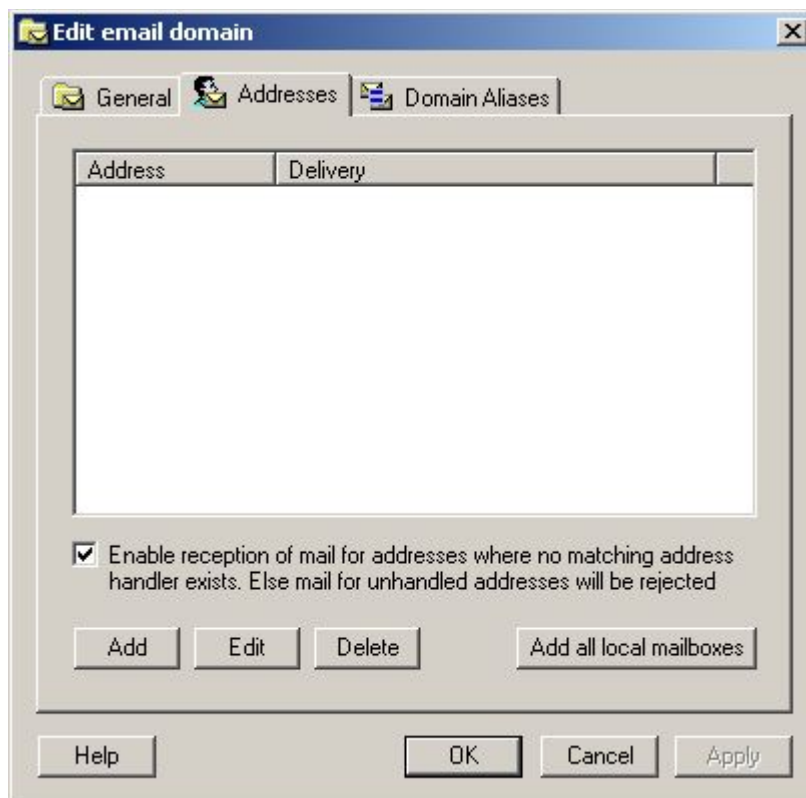
Open the Email properties from the 'System Services' tab in GateKeeper, and the following screen will appear. The domain of the email that is to be hosted now needs to be entered, click Add. (*The Domain you enter needs to have a DNS record located somewhere (either locally by you, or with your service provider)).



Upon clicking Add the following screen appears, and it is here that Domain specific properties can be set. The General tab indicates whether this new domain is hosted locally or on another server. As WinGate in this scenario, is acting as the primary mail server for the network, 'Mailboxes for this domain are hosted on this server' should be selected.



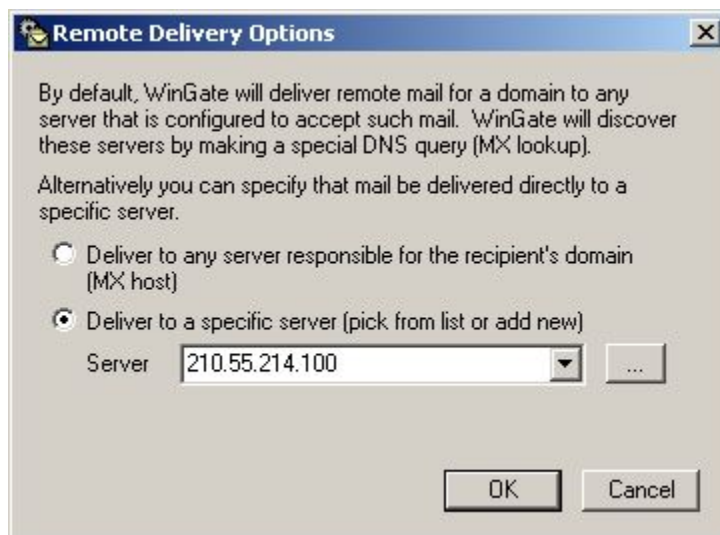
Next on the Addresses tab, email handlers need to be added to the domain, as it is these two pieces of information (the email handler and the domain) that create the email address. (For more information about Email Handlers see above) This is where this scenario deviates from the standard set-up. As the Head Office will be receiving mail for both local and remote (Provincial Office) users, there needs to be two different styles of Email Handler configured. Firstly, for local users at the Head Office, the default option 'To enable reception of mail for addresses where no matching address handler exists' should be left ticked as this setting means that when WinGate receives an email, it will see that there are no email handlers listed, and so will check the user database (be it NT or the WinGate DB) and if a match is found with a user account that is enabled for email then the mail will be accepted and delivered. So for example, if the user bob has been created as a user in WinGate, and an email is received for bob@qbik.com (presuming that qbik.com is the domain that is being locally hosted), then WinGate will see there is no message handler for bob, but as this option is ticked it will check the user database to see if bob exists there, and as he does, WinGate will accept the email. If mailboxes are being hosted locally then each user on the Head Office LAN will require a local user account in WinGate (be it NT or the WinGate DB).



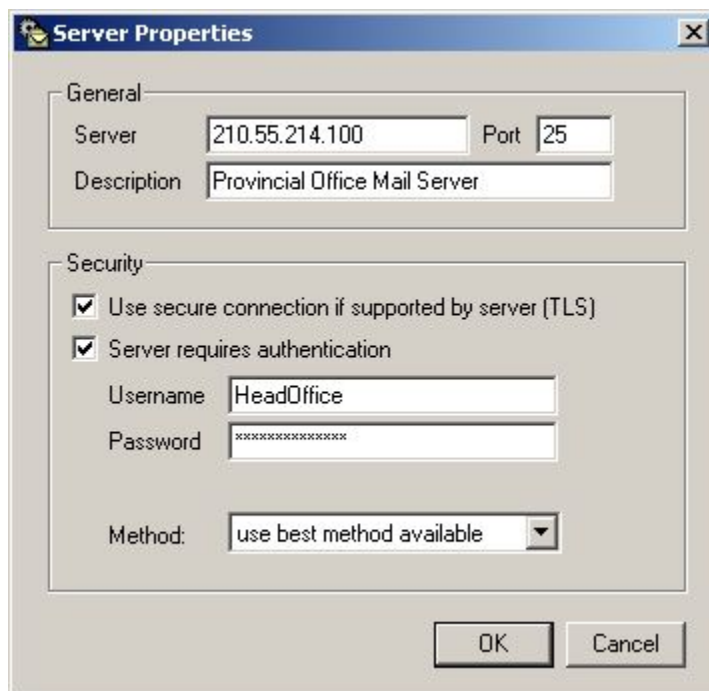
However, for users at the remote (Provincial) location, Email Handlers HAVE to be added (see above), so that mail for these users is pushed (forwarded) on to the Provincial Office's mail server. To create a new email handler for a remote user click Add. Once the user address has been specified (in this case Jim), the domain's default delivery settings need to be overridden and 'Deliver mail to another mail server' needs to be selected. The Destination should then be set with the same email address that the Head Office mail server would have accepted when it received the email. This presumes that the Provincial Office is using the same domain as the Head Office, which would usually be the case in this scenario. Next, click the '...' button to specify the remote (Provincial Office) server .



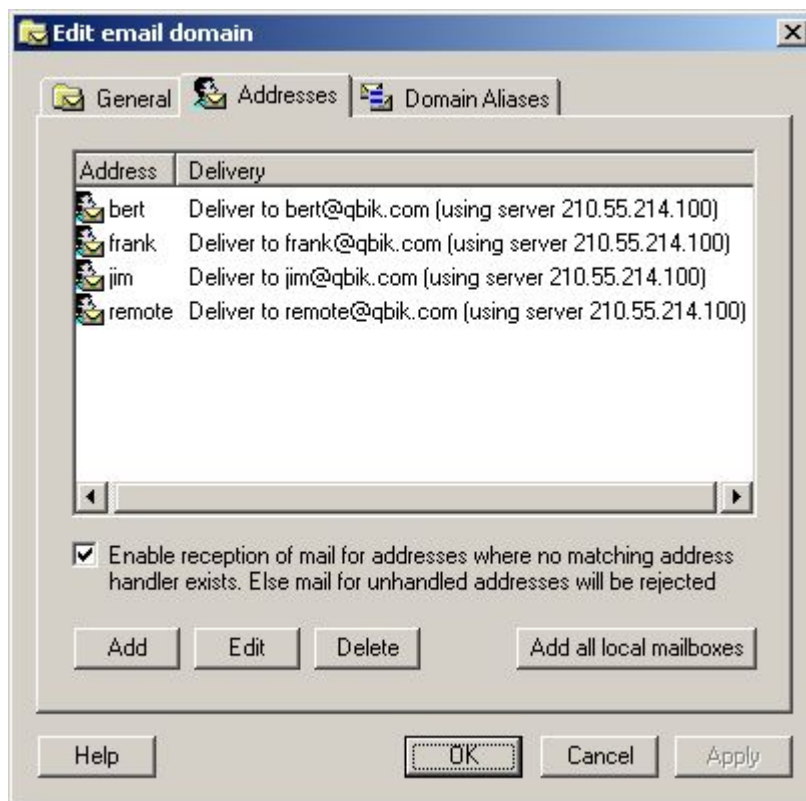
The option 'Deliver to a specific server' should be selected here. If the deliver to MX host option was selected this could cause a mail loop, as the MX host responsible is this Head Office server. Either the IP or the domain name (if it has one) of the remote (Provincial) server can be entered. As the Provincial Office wont be receiving email from random internet mail servers (i.e. only this Head Office server will be sending to it) then 'good practice' would be for the remote server to require authentication to access it's SMTP server. There are a number of different authentication methods the Head Office can use to connect to the Provincial Office, and these can be accessed by clicking the '...' button.



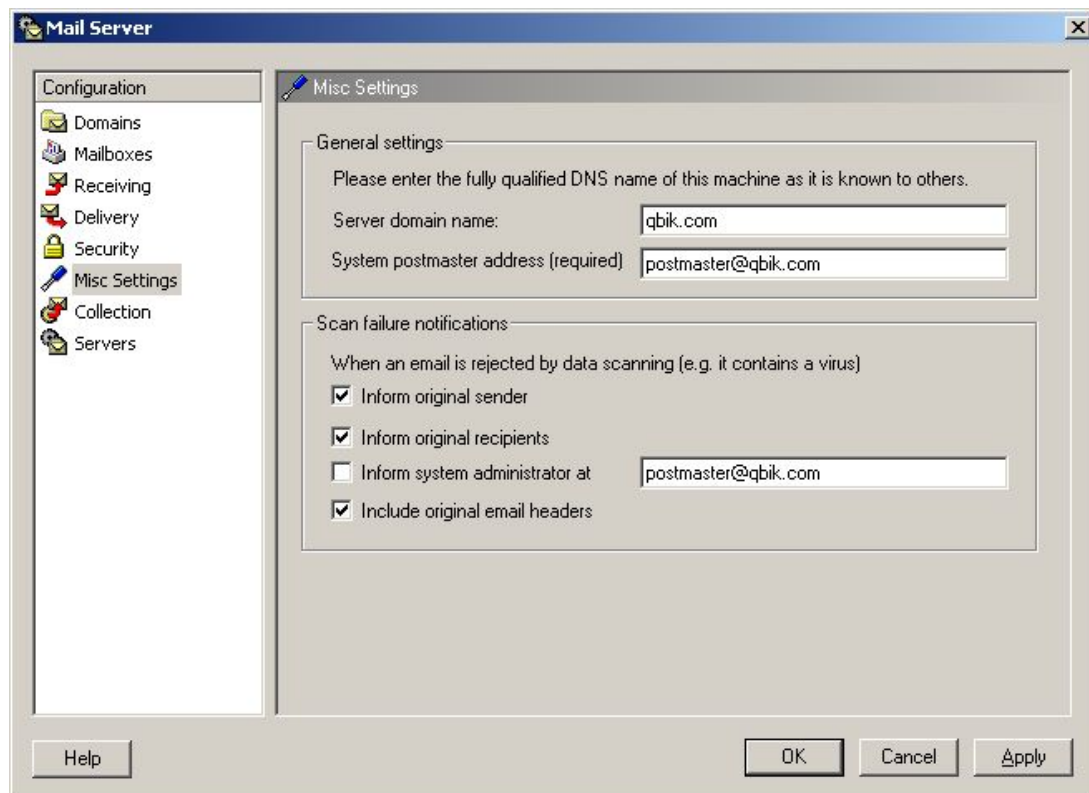
The General options are fairly straightforward with the server name / IP, the port it is listening on, and a text description (if required of the remote server). By default the security options allow for the use of TLS connections (if the remote server supports them, which WinGate does). Then there is the choice of authentication method to use when connecting to the remote (Provincial) server. The default of 'best method available' is satisfactory, as WinGate will determine what methods the remote server supports, and use the most secure. However, if the remote authentication method is known, then it can be manually specified, from a choice of SASL PLAIN, CRAM-MD5, and NTLM. A valid username and password that allows access to the remote server should also be specified. In this scenario where the remote server is also running WinGate Mail, this username and password would be a user account that exists on the remote server. (For more information regarding WinGate mail security see <http://www.wingate.com/resources.php?id=12>)



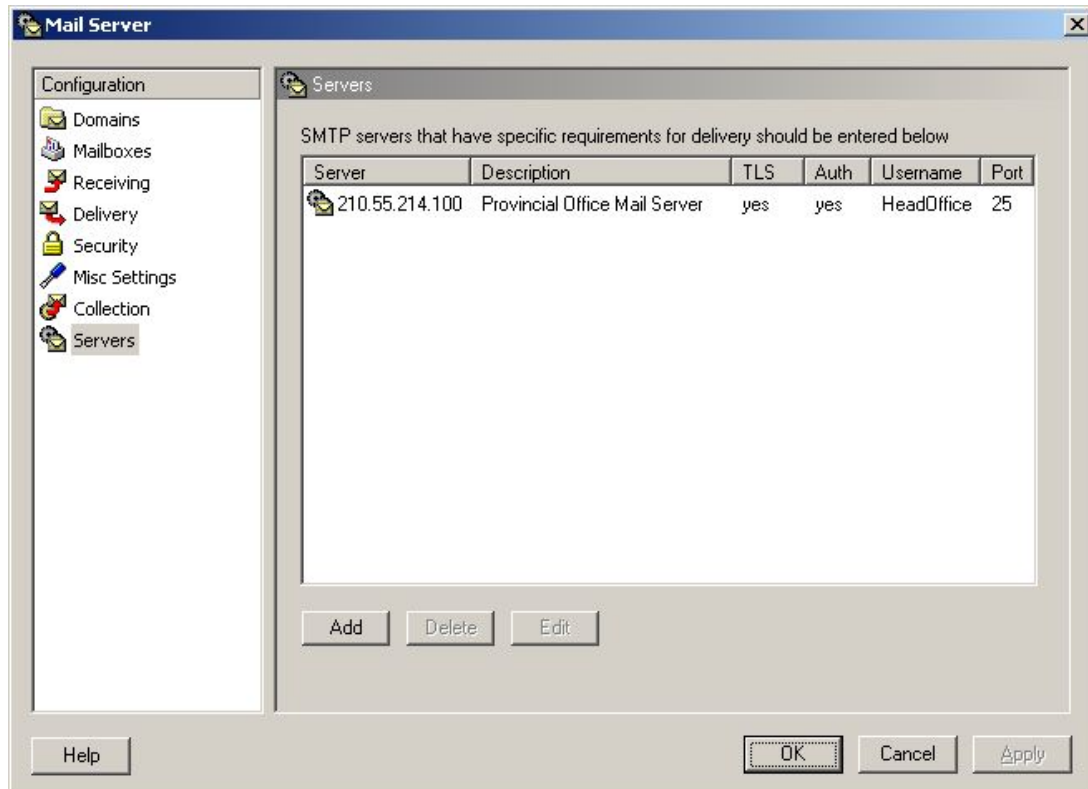
Once the specific server properties have been detailed, click OK back out to the main Email Handler screen. For all additional Handlers that are added, the remote server should be available from the drop down list on the Remote Delivery Options dialog, to make configuring multiple remote users to the same server quick and easy.



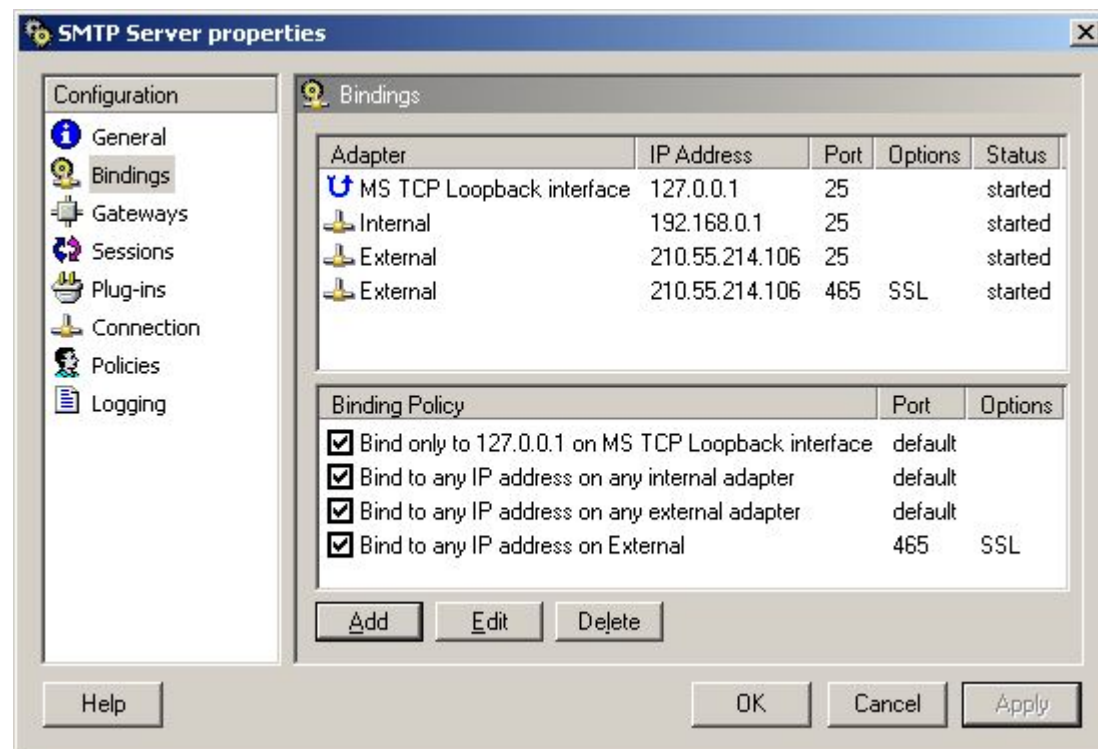
The majority of the other settings can be left on the defaults, and tweaked as desired, except for under the Misc Settings, where the Server Domain Name, and the System Postmaster Address MUST be filled out correctly, otherwise mail originating from this server maybe rejected by other mail servers on the internet. The Scan failure notifications configuration is only important if you have Anti Virus for WinGate installed.



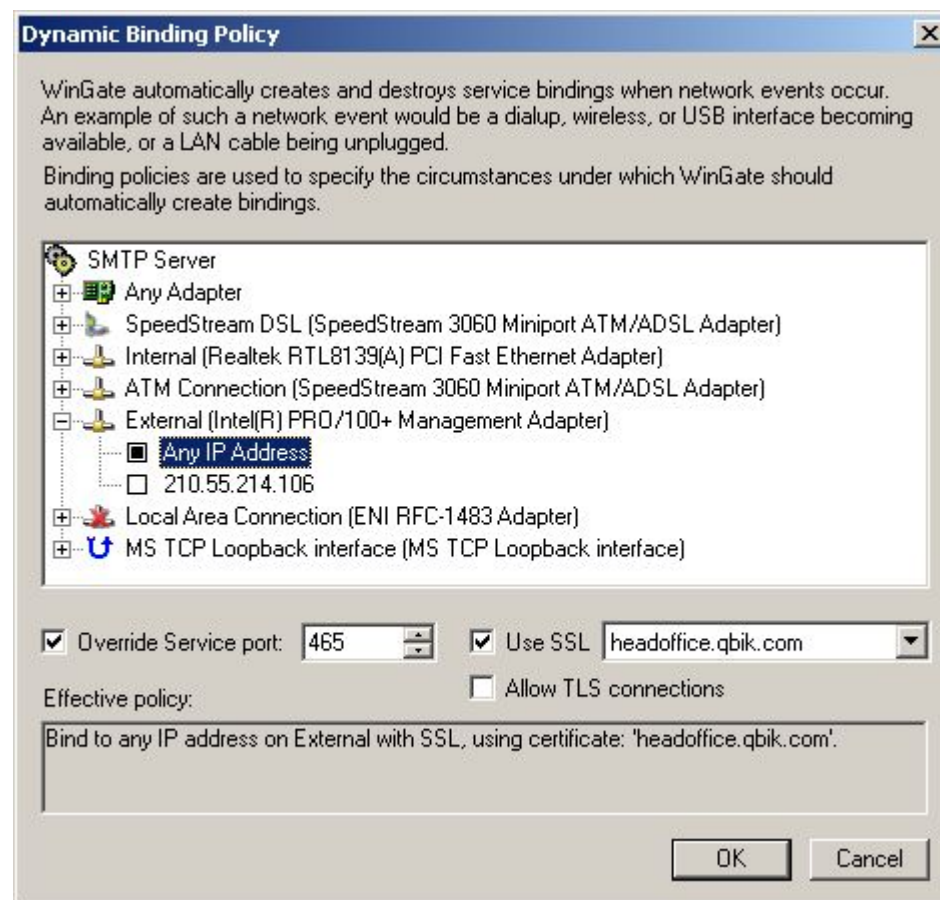
The remote (Provincial) server that was specified as the delivery override for each unique Email Handler, can be viewed and edited from the Servers pane in the Mail Server properties. Any additional servers that the Head Office may want to deliver to secure can be added here. Before WinGate tries to deliver to a domain, be it for an Email Handler override, or just plain delivery to a mail server on the internet, it will check the list of server's here first to see if there are any specific delivery requirements.



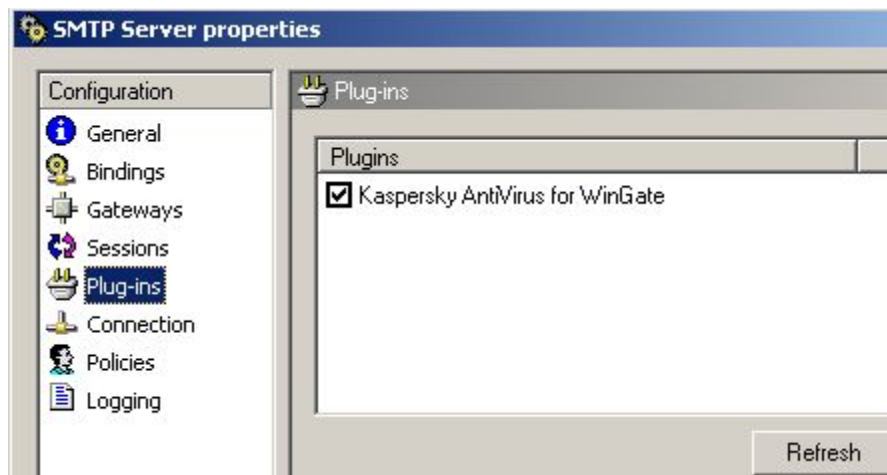
Now that the Head Office mail server configuration is complete, the only other area of WinGate that needs to be configured is the SMTP bindings. For safety reasons a default install of WinGate only binds services to trusted / internal interfaces, but when setting up WinGate for email, the bindings for SMTP have to be modified so that WinGate can receive emails sent to the domain it is hosting from elsewhere on the internet. In this scenario mail is pushed from the Head Office down to Provincial Office, and vice versa. For extra security of this communication, it can take place over a secured SSL connection. From GateKeeper open the SMTP properties on the System tab.



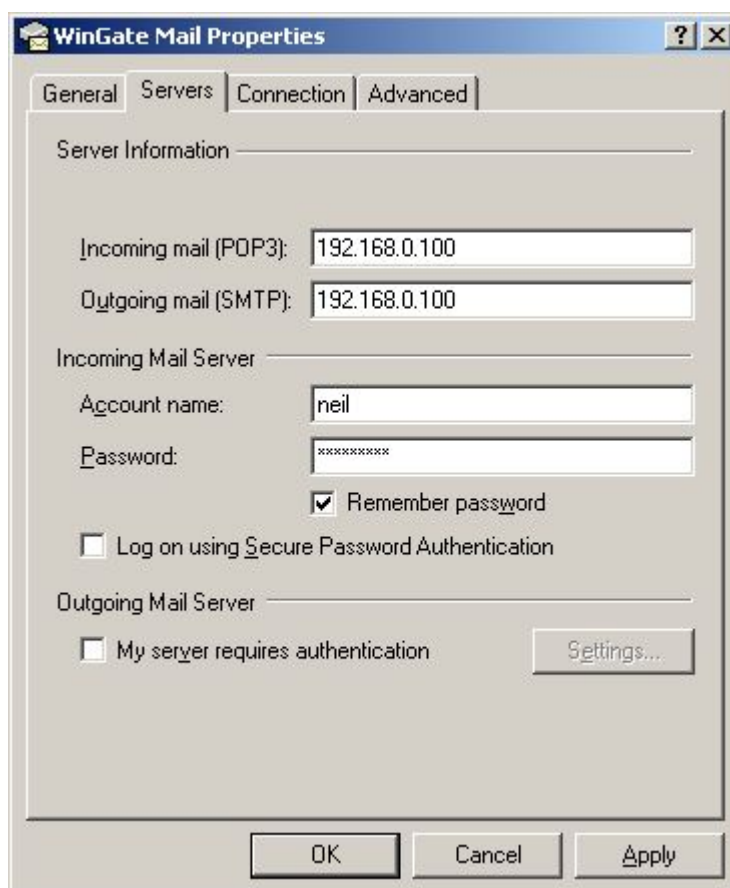
Next click Add to create a new Bindings Policy. Two new policies should be created, one for standard SMTP connections, and one for secure SSL connections from the remote office. For a standard binding, create a new policy for the External adapter for 'Any IP Address'. The other options here are for advanced users so the defaults can be left as they are. However, to create an advanced bindings policy, some more options need to be configured. The adapter options can either be set as for a standard binding, or the option to use 'Any IP' on 'Any Adapter' could be selected as this binding policy will use a different port to any previously configured, and thus there will be no port conflicts. So in addition the Override Service port option should be set to 465, with the Use SSL option ticked, and an appropriate certificate selected. (For more information about Certificates in WinGate see the Help file).



Finally, if you have any WinGate Anti-Virus product installed, check to make sure the Anti-Virus scanning is enabled in the SMTP Server properties.



WinGate is now configured to act as the primary mail server at the Head Office. The next step is to configure the email clients on the LAN, such as Outlook, Outlook Express, or The Bat etc. These Client machines then need to have their SMTP and Pop3 settings pointed to the WinGate machine's IP address. This example shows the entries that would be made in Outlook Express if the Head Office WinGate server's IP was 192.168.0.100.



This example shows the entries that would be made in The Bat if the Head Office WinGate server's IP was 192.168.0.100.

Account Properties - WinGate 6 Mail

Send mail

SMTP Server: 192.168.0.100 Authentication...

Connection: Regular Port: 25

Receive mail

Mail Server: 192.168.0.100 Authentication...

User: bob Password: Password masked Protocol: POP3

Connection: Regular Port: 110

Delivery

☒ Immediate ☐ Deferred

☐ Combined delivery (send+receive)

OK Cancel Help

This example shows the entries that would be made in Outlook XP if the Head Office WinGate server's IP was 192.168.0.100.

E-mail Accounts

Internet E-mail Settings (POP3)

Each of these settings are required to get your e-mail account working.

User Information

Your Name: bob

E-mail Address: bob@qbik.com

Server Information

Incoming mail server (POP3): 192.168.0.100

Outgoing mail server (SMTP): 192.168.0.100

Logon Information

User Name: bob

Password: Password masked

☒ Remember password

☐ Log on using Secure Password Authentication (SPA)

Test Settings

After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

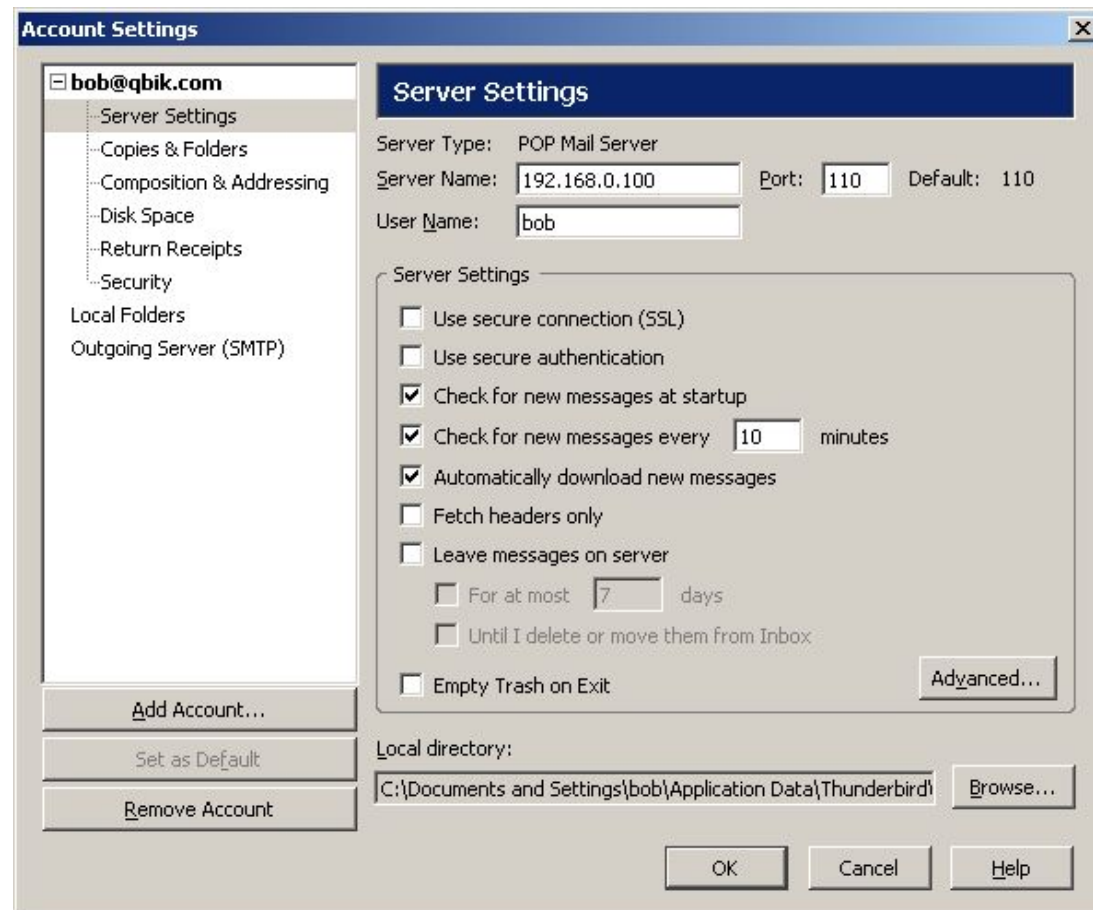
Test Account Settings ...

More Settings ...

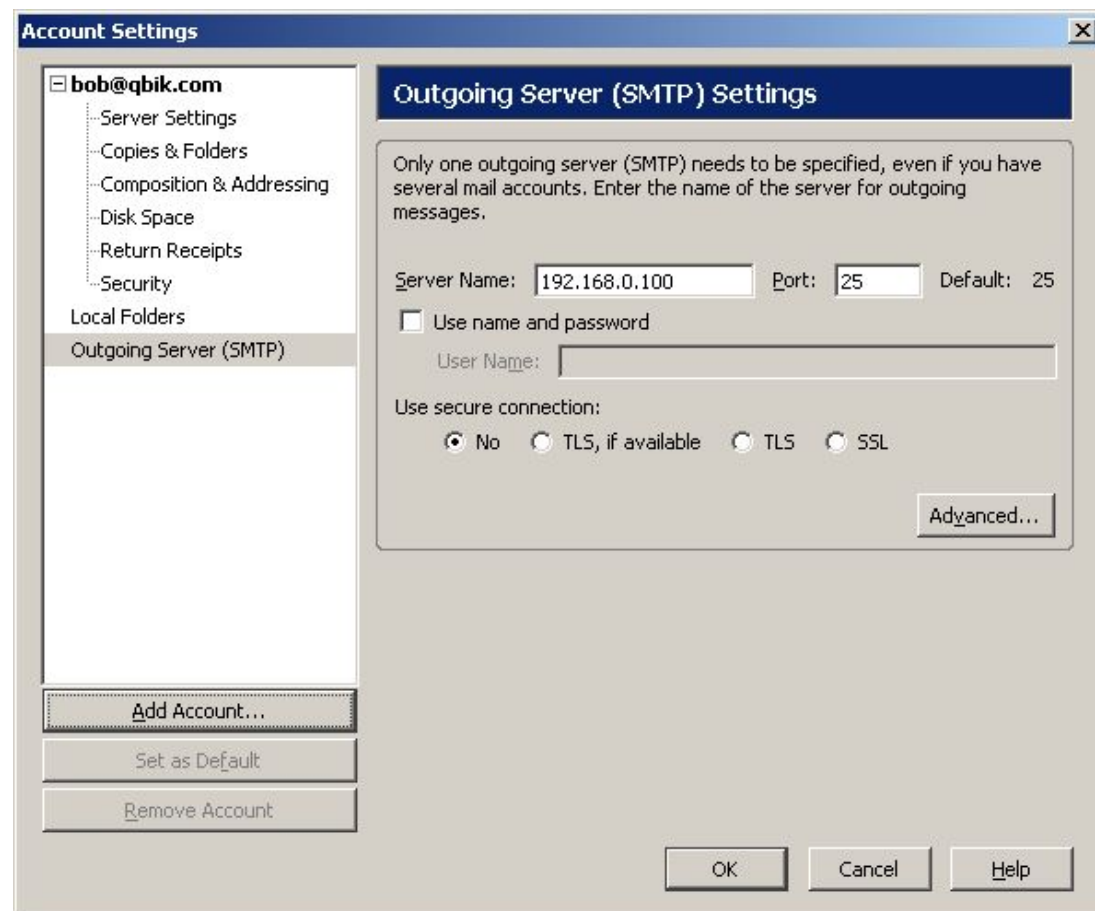
< Back Next > Cancel

This example shows the entries that would be made in Thunderbird if the Head Office WinGate server's IP was 192.168.0.100.

Firstly POP3:



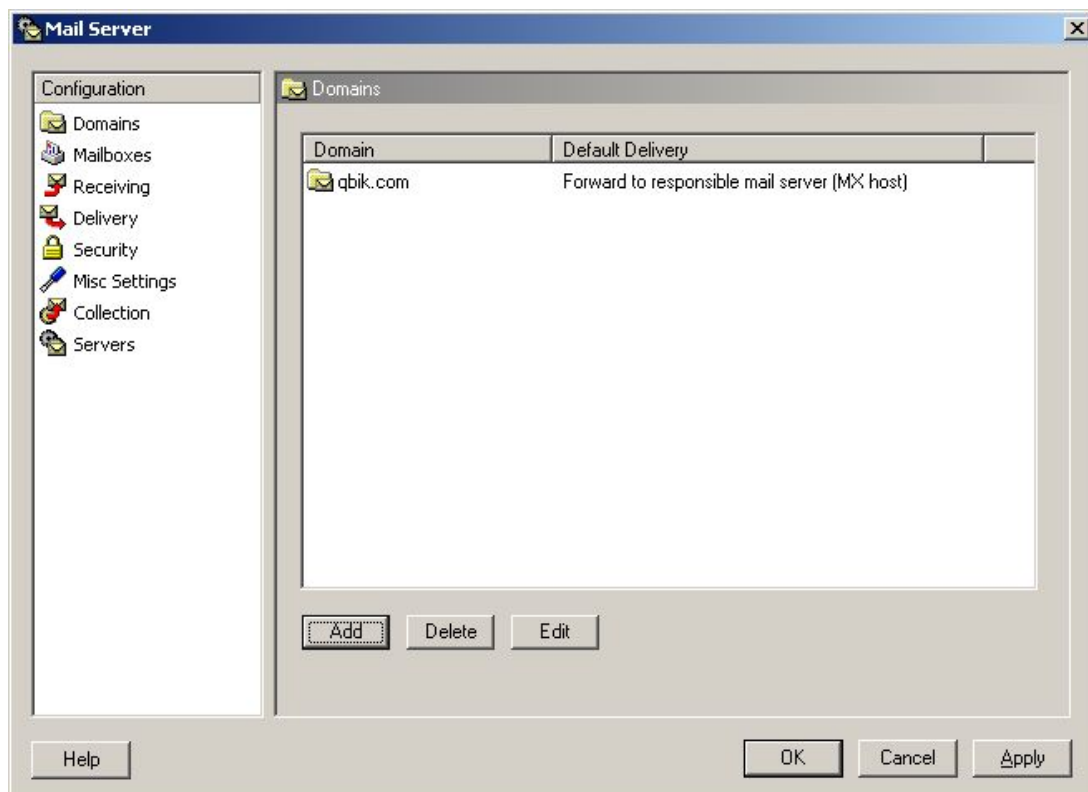
Then SMTP:



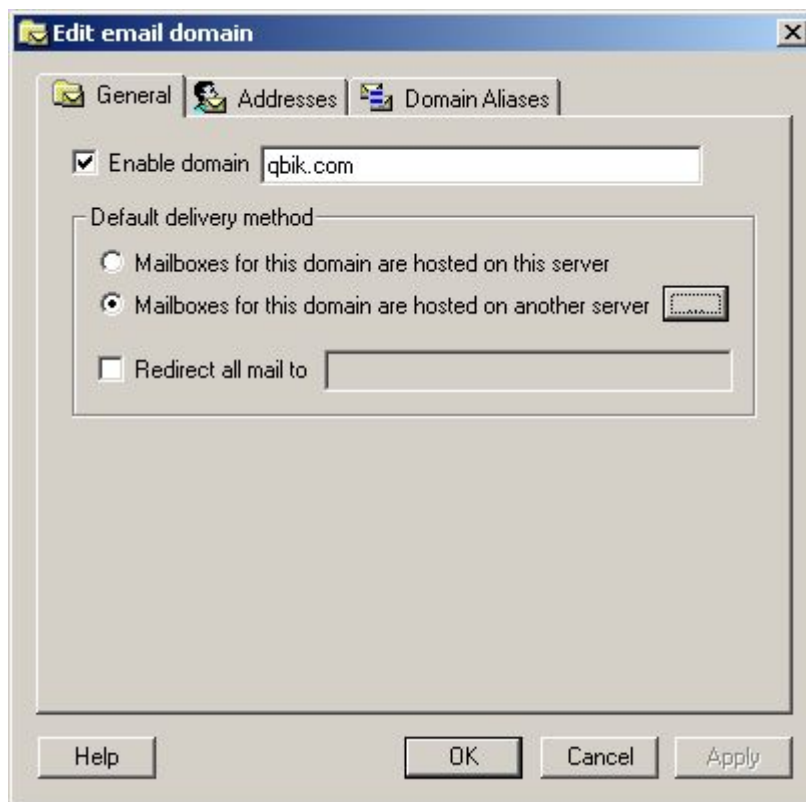
Remote (Provincial) Office WinGate Mail Configuration

The remote office set-up is very similar to the WinGate set-up in scenario 3 when the ISP hosts the mail for the domain. The key differences this time are that the Head Office hosts the mail, and instead of this remote office retrieving the mail via POP Collection, it is pushed down from the Head Office, via SMTP.

Open the Email properties from the 'System Services' tab in GateKeeper, and under the Domains option, click Add. Enter the name of the domain that is hosted on the Head Office's mail server. Here it is qbik.com. Even though this WinGate at the remote office isn't hosting the domain, it still needs to know what your domain is called, so that it will only allow email from your domain to be sent.



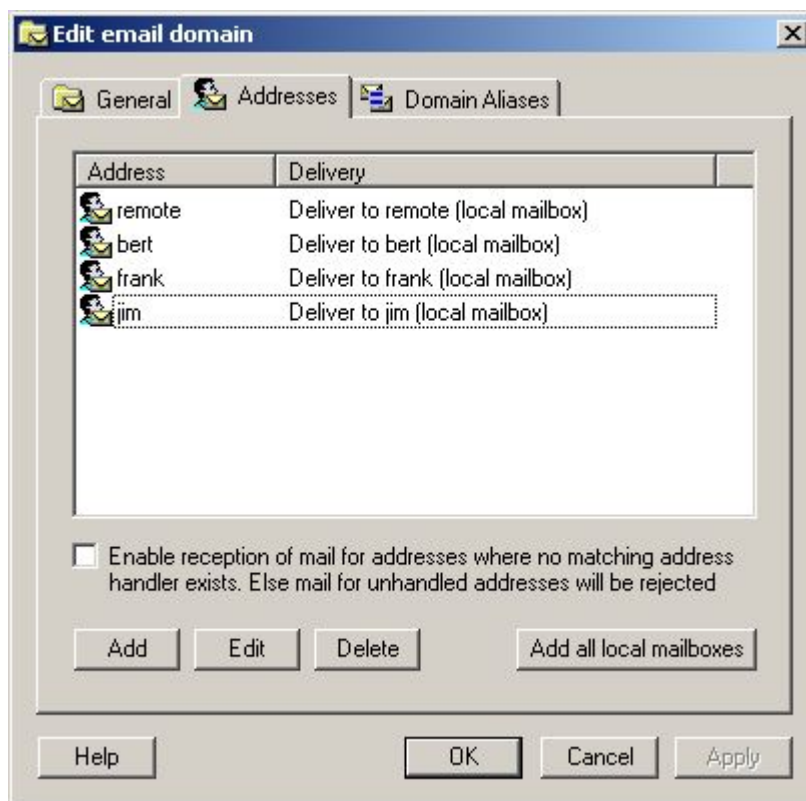
Upon entering the domain name, WinGate then needs to be told that it isn't the primary mail server for the network, so move the radio button to 'Mailboxes for this domain are hosted on another server', and click the '...' button at the end of the line.



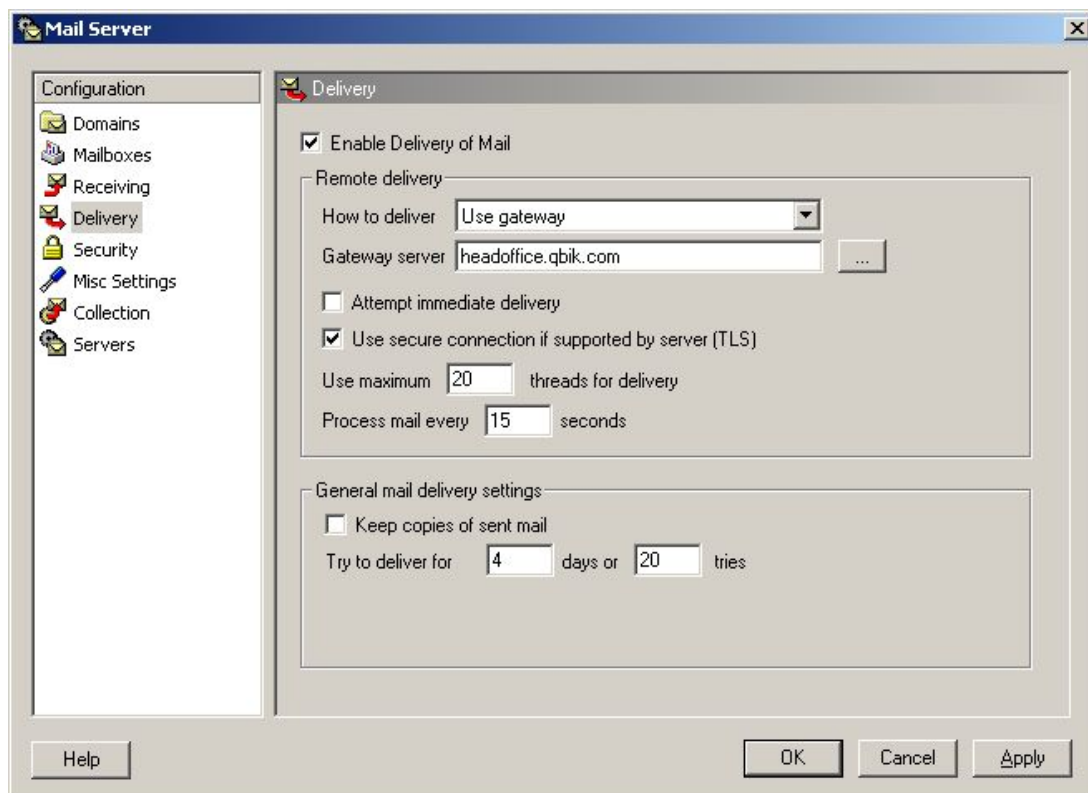
As the Head Office is hosting the domain, the DNS MX record for it will be pointing there, and so the top option should be left selected. Click OK.



The Email handlers need to be configured on the addresses tab. The default option of 'Enable reception of mail for addresses where no matching address handler exists' should be UNTicked. This is because most mail for this domain should be sent to / held by the Head Office server. For example, if Jim is a worker at the Provincial Office, and wants to send an email to Bob at Head Office then having this option UNTicked makes sure that the mail is sent on to the Head Office server, rather than attempting to deliver the mail locally, which would fail as there isn't a mailbox for Bob on this remote (Provincial) server. However, in addition to removing this default option, local Email Handler overrides need to be created so that mail that is destined for users with accounts /mailboxes on this Provincial server, is accepted and not rejected or forwarded on to the Head Office server unnecessarily. For another example, if Jim wants to send an email to Frank, they are both based at this Provincial Office, so WinGate needs to be told that this email does not need to be forwarded on to the Head Office server, but instead delivered locally, which is what the Email Handler override for Frank specifies.



The delivery pane options need to be configured next. This is not actually compulsory, as this remote server could be left on the default setting to deliver all mail directly to its destination. However this scenario is presuming that there is a company policy that all outbound (internet) mail must go out through the Head Office server. In this case, the 'Remote delivery' option of 'How to deliver' should be set to 'Use gateway' and the Head Office server's domain name, or IP address, should be entered. As authentication with the Head Office server will be required, click the '...' button.



As before in the Head Office set-up, the General options are fairly straightforward with the server name / IP, the port it is listening on, and a text description (if required). By default the security options allow for the use of TLS connections (if the remote server supports them, which WinGate does). Then there is the choice of authentication method to use when connecting to the Head Office server. The default of 'best method available' is satisfactory, as WinGate will determine what methods the remote server supports, and use the most secure. However, if the remote authentication method is known, then it can be manually specified, from a choice of SASL PLAIN, CRAM-MD5, and NTLM. A valid username and password that allows access to the Head Office server should also be specified. In this scenario where the Head Office server is also running WinGate Mail, this username and password would be a user account that exists on the Head Office server. (For more information regarding WinGate mail security see <http://www.wingate.com/resources.php?id=12>)

Server Properties

General

Server: Port:

Description:

Security

☒ Use secure connection if supported by server (TLS)

☒ Server requires authentication

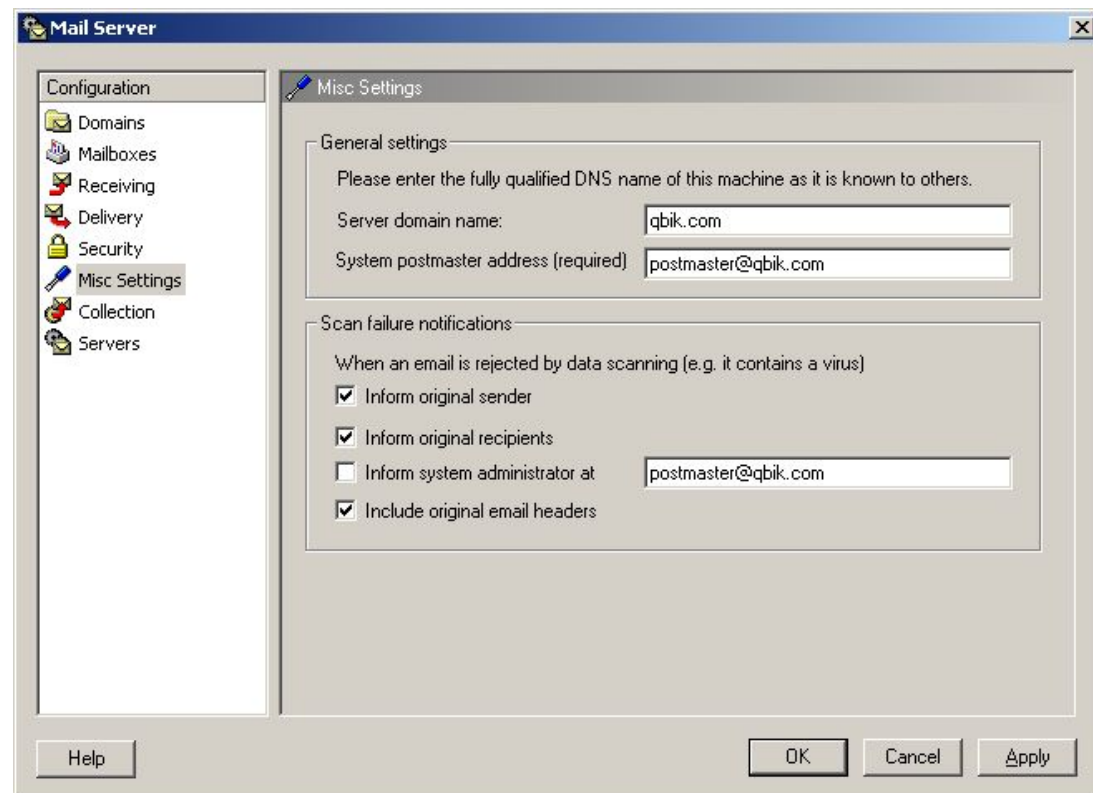
Username:

Password:

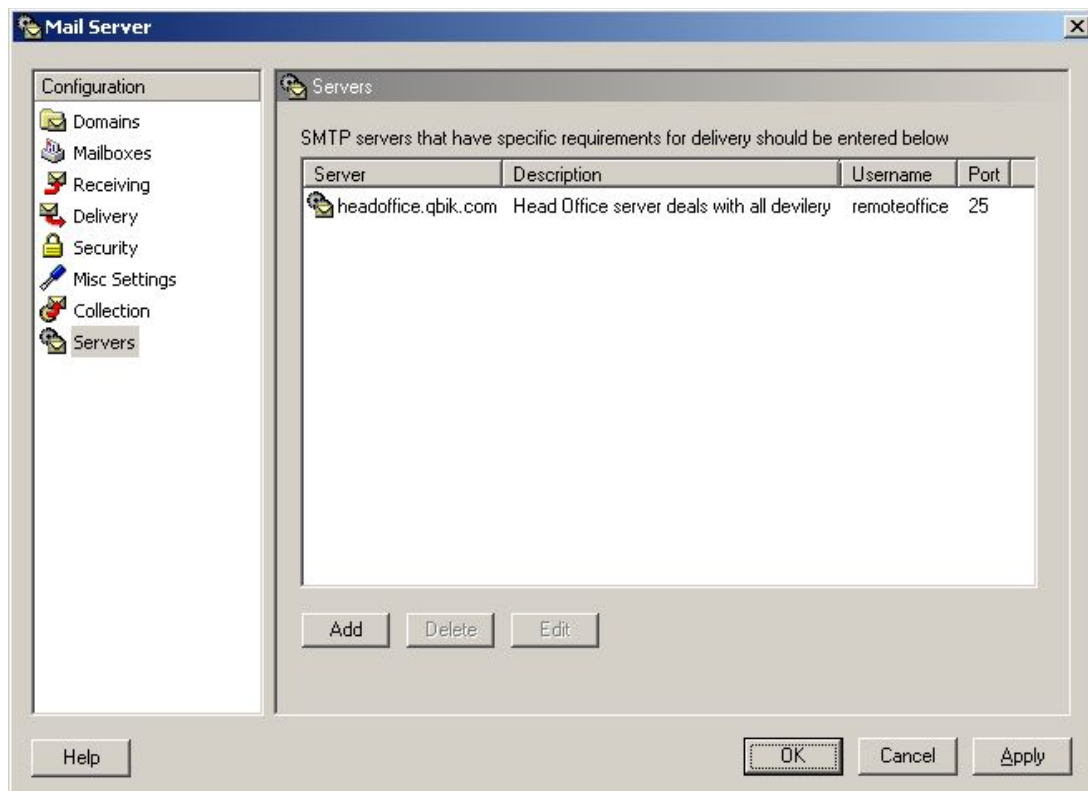
Method:

OK Cancel

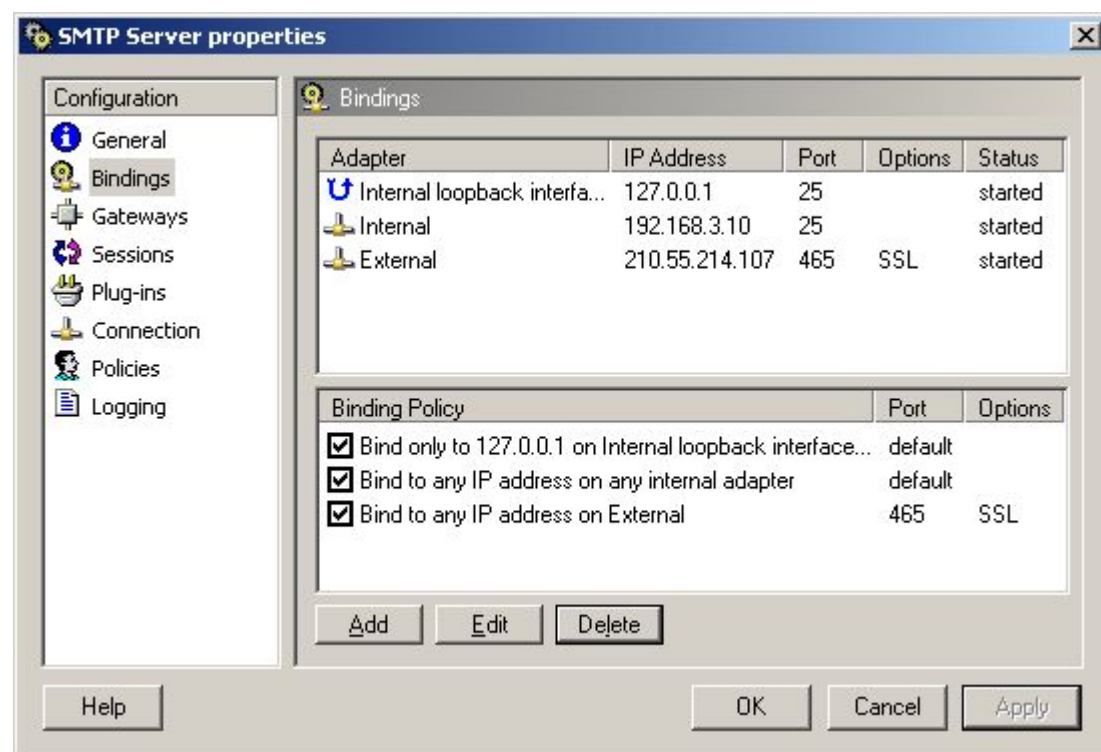
Under the Misc Settings, the Server Domain Name, and the System Postmaster Address MUST be filled out correctly, otherwise mail originating from this server maybe rejected. Although not as important at this Provincial Office as at the Head Office (as this remote server will authenticate with the Head Office server anyway), completing this section is still a requirement. The Scan failure notifications configuration is only important if you have Anti Virus for WinGate installed.



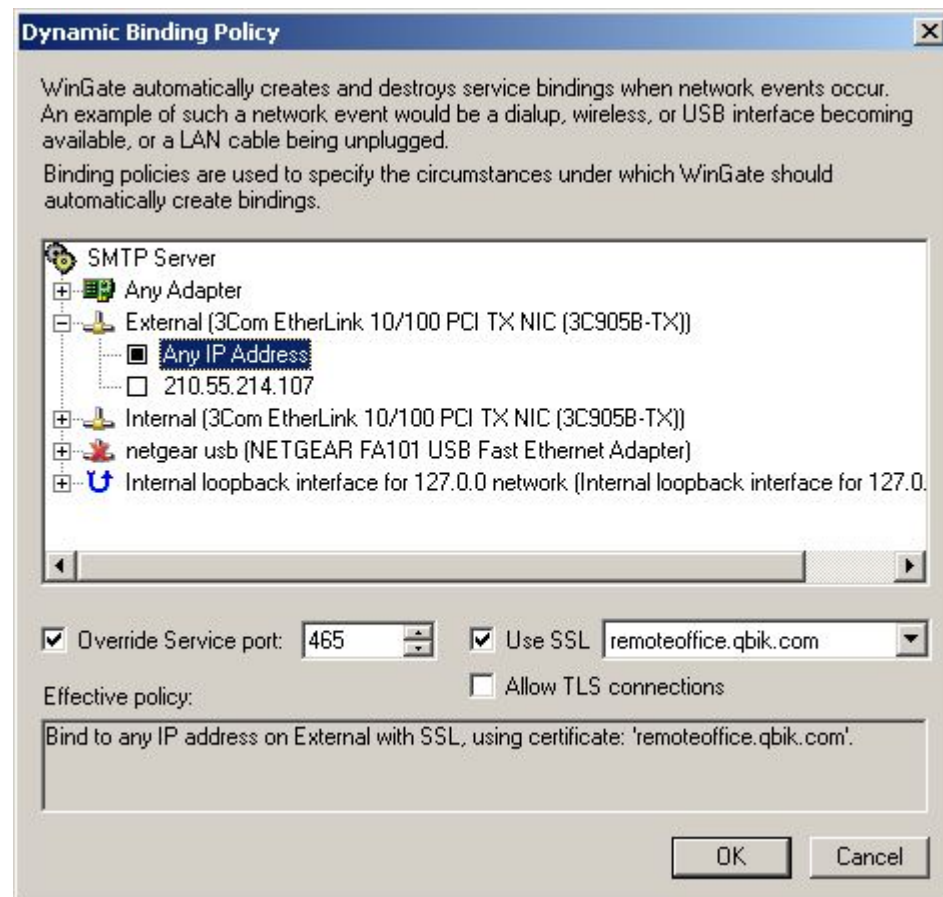
The server that was configured in the Delivery pane, can be viewed, and re-configured if necessary under the Server's pane in the Mail server properties.



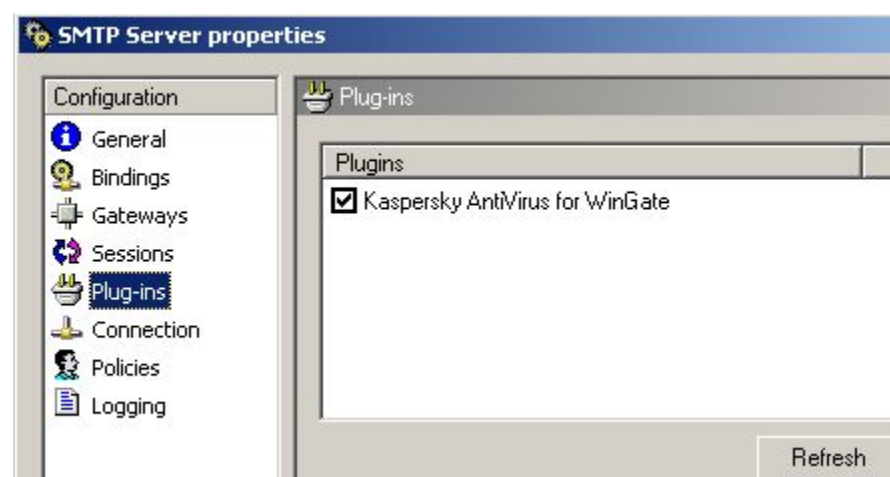
Now that the Provincial Office mail server configuration is complete, the only other area of WinGate that needs to be configured is the SMTP bindings. For safety reasons a default install of WinGate only binds services to trusted / internal interfaces. In this scenario mail is pushed from the Head Office down to Provincial Office, and vice versa, and thus a standard binding on port 25 is not required (although could be added). The binding policy that should be created here is a secure one that will only receive from the Head Office. From GateKeeper open the SMTP properties on the System tab.



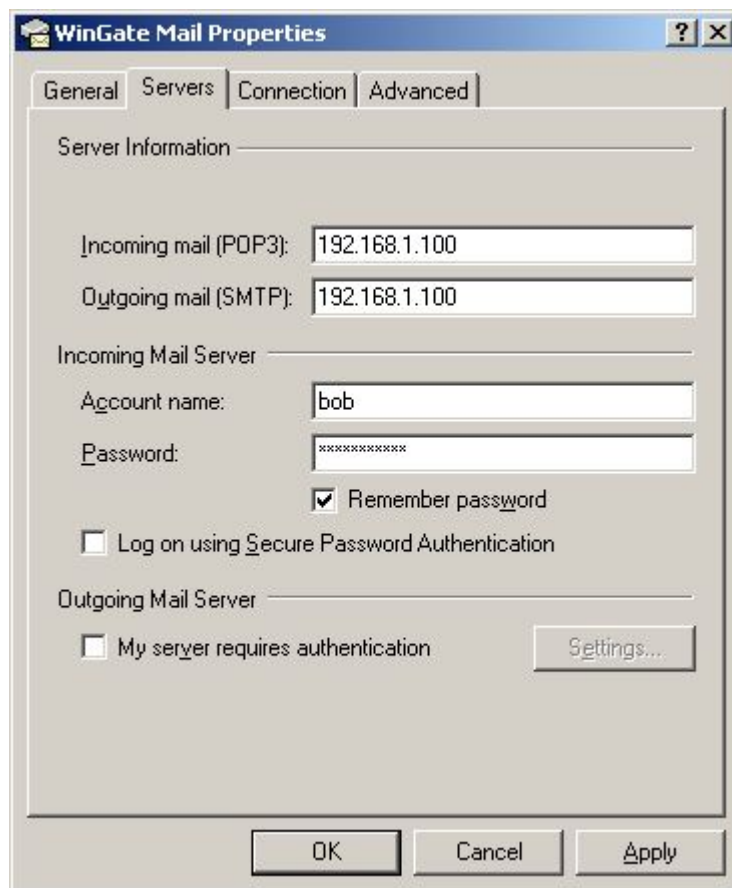
Next click Add to create a new Bindings Policy. To create an advanced bindings policy, the adapter options can either be set as for a standard binding (i.e. specifying a particular adapter), or the option to use 'Any IP' on 'Any Adapter' could be selected as this binding policy will use a different port to any previously configured, and thus there will be no port conflicts. So in addition the Override Service port option should be set to 465, with the Use SSL option ticked, and an appropriate certificate selected. (For more information about Certificates in WinGate see the Help file).



Finally, if you have any WinGate Anti-Virus product installed, check to make sure the Anti-Virus scanning is enabled in the SMTP Server properties.



WinGate Mail is now configured for the Provincial Office network. The next step is to configure the email clients on the remote office LAN, such as Outlook, Outlook Express, or The Bat etc. These Client machines then need to have their SMTP and Pop3 settings pointed to this Provincial Office WinGate machine's internal IP address (not the Head Office mail server's IP as WinGate will take care of the forwarding). This example shows the entries that would be made in Outlook Express if the Provincial Office WinGate server's IP was 192.168.1.100.



The image shows a screenshot of the 'WinGate Mail Properties' dialog box. It has four tabs: 'General', 'Servers', 'Connection', and 'Advanced'. The 'General' tab is selected. The 'Server Information' section contains two text boxes: 'Incoming mail (POP3):' with the value '192.168.1.100' and 'Outgoing mail (SMTP):' with the value '192.168.1.100'. The 'Incoming Mail Server' section contains 'Account name:' with the value 'bob', 'Password:' with a masked password 'xxxxxxxx', and a checked checkbox for 'Remember password'. There is also an unchecked checkbox for 'Log on using Secure Password Authentication'. The 'Outgoing Mail Server' section contains an unchecked checkbox for 'My server requires authentication' and a 'Settings...' button. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

WinGate Mail Properties

General Servers Connection Advanced

Server Information

Incoming mail (POP3): 192.168.1.100

Outgoing mail (SMTP): 192.168.1.100

Incoming Mail Server

Account name: bob

Password: xxxxxxxxxx

☒ Remember password

☐ Log on using Secure Password Authentication

Outgoing Mail Server

☐ My server requires authentication

Settings...

OK Cancel Apply

This example shows the entries that would be made in The Bat if the Provincial Office WinGate server's IP was 192.168.1.100.

Account Properties - WinGate 6 Mail

General

Send mail

SMTP Server: 192.168.1.100 Authentication...

Connection: Regular Port: 25

Receive mail

Mail Server: 192.168.1.100 Authentication...

User: bob

Password: Password masked Protocol: **POP3**

Connection: Regular Port: 110

Delivery

☒ Immediate ☐ Deferred

☐ Combined delivery (send+receive)

OK Cancel Help

This example shows the entries that would be made in Outlook XP if the Provincial Office WinGate server's IP was 192.168.1.100.

E-mail Accounts

Internet E-mail Settings (POP3)

Each of these settings are required to get your e-mail account working.

User Information

Your Name: bob

E-mail Address: bob@qbik.com

Server Information

Incoming mail server (POP3): 192.168.1.100

Outgoing mail server (SMTP): 192.168.1.100

Logon Information

User Name: bob

Password: Password masked

☒ Remember password

☐ Log on using Secure Password Authentication (SPA)

Test Settings

After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

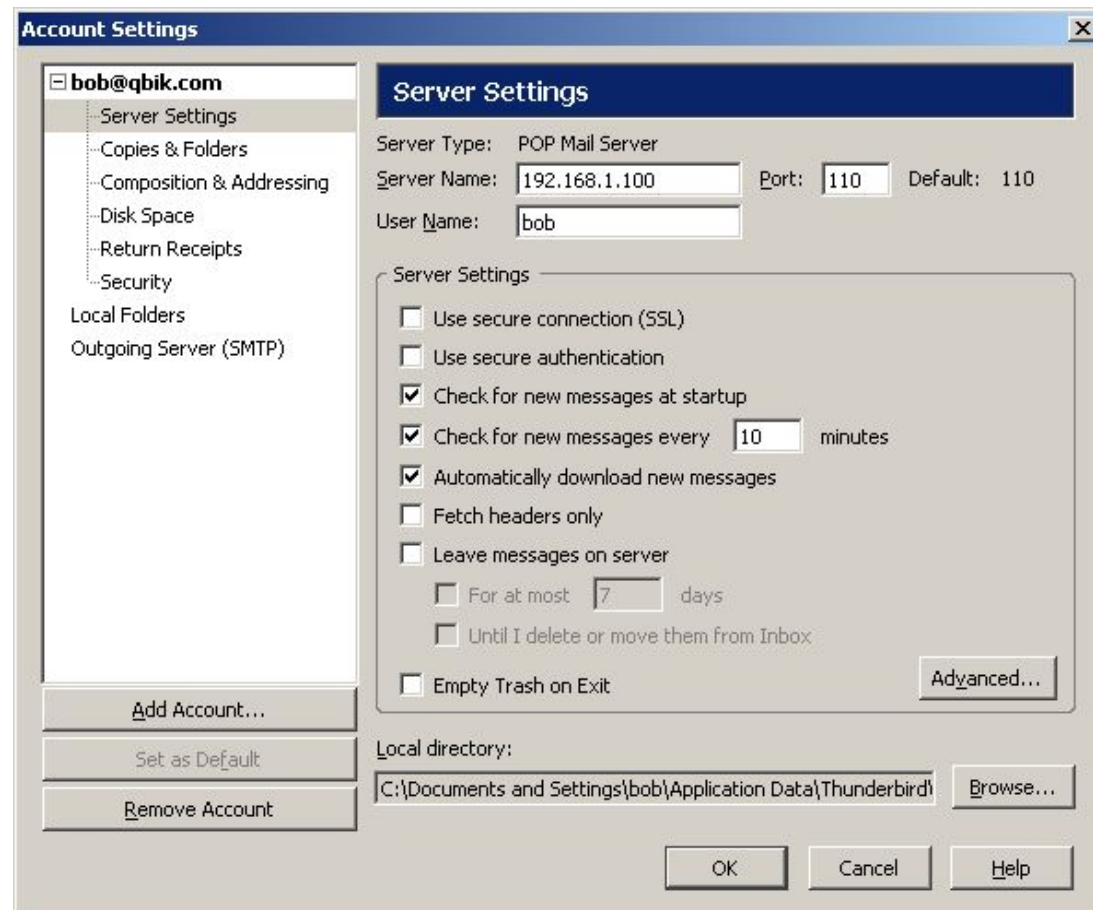
Test Account Settings ...

More Settings ...

< Back Next > Cancel

This example shows the entries that would be made in Thunderbird if the Provincial Office WinGate server's IP was 192.168.1.100.

Firstly POP3:



Then SMTP:

