# Welcome to **InvisiMail 3.1**

Congratulations on choosing RPK InvisiMail, the global high strength solution for secure e-mail communications on the Internet.

RPK InvisiMail is an **easy-to-use** e-mail security enhancement for use with all standards-compliant Internet e-mail clients and servers. Certified by the International Computer Security Association, InvisiMail automatically and transparently encrypts e-mail messages and attachments, authenticates the sender and verifies the contents have not changed in transit.

**Transparent to the user**
InvisiMail works in the background. No special buttons, menu commands or other procedures are added or required. You don't need to know anything about encryption. RPK InvisiMail handles everything for you. All you need to do is choose and remember a password. Then just send and receive e-mail as you normally do.

**Automatic key management**
Each time you send a message, your public key is embedded in the header of the message, therefore, the way you send your key to another RPK InvisiMail user is simply by sending them a message. Once a recipient's key has been received, all future messages to them are encrypted.

**Automatic encryption**
RPK InvisiMail automatically encrypts the entire message including attachments. You never have to remember to issue commands to encrypt, thus eliminating the possibility of user error in highly secure environments. With RPK InvisiMail, all the benefits of e-mail security become automatic and transparent. Older systems that required user interaction were designed that way because they were too slow and therefore took too much time to encrypt every message. Since RPK InvisiMail is so fast, there is very little overhead incurred when encrypting messages and so encrypting all messages is not a burden.

RPK InvisiMail is also intelligent in deciding who can receive encrypted message and who cannot. RPK InvisiMail can only encrypt a message to a recipient from whom it has already received the public key. Therefore, it will only send encrypted messages to other users of InvisiMail. Otherwise it will send the message unchanged and clearly readable by the intended recipient.

**Easiest-to-use**
InvisiMail handles everything automatically. It's the easiest-to-use e-mail encryption package available today.

**Multi-platform support**
InvisiMail supports more Internet e-mail software than any other product in its category. If you are already using one of the major e-mail software products such as Netscape (Navigator or Communicator), Microsoft Internet Explorer (Internet Mail or Outlook Express), Microsoft Exchange or Outlook, Eudora (Light or Pro), Calypso, Pegasus or TurnPike you simply install RPK InvisiMail and everything is taken care of automatically. Should you be using a different SMTP/POP3 compliant system it is still possible to install RPK InvisiMail by manually configuring the settings in your e-mail software.

**Globally strong encryption you can trust**
InvisiMail is the first e-mail security product with globally strong encryption that is directly available from the original developer. InvisiMail uses the RPK Fast Public Key Encryptonite™ Engine, developed by

RPK New Zealand Ltd., the strongest cryptography available worldwide today. Because the underlying RPK encryption algorithm and the product were both developed outside the United States, InvisiMail is not subject to the well publicized U.S. export restrictions on strong encryption.

### FREE InvisiMail Intro version

As an InvisiMail user, you can send the FREE InvisiMail Intro version to anyone worldwide, providing compatibility and security for all your e-mail messages, without requiring others to purchase anything.

## RPK InvisiMail Features

Automatically:-

- *Encrypts* messages including attachments
- *Authenticates* the sender of each message
- *Validates* that the contents of each message have not changed in transit
- *Maintains* keys used for encryption and authentication

Uses patented high-strength encryption, available on a worldwide basis for all e-mail messages and attachments.

Two levels of security:-

- Strong (607 bits)
- Extreme (1279 bits)
- Compression to reduce message size, transmission time and increase security
- FREE InvisiMail Certificate provided for all Deluxe and Enterprise users

MIME Internet standard compatible

- Supports X.509 style certificates
- Supports 3rd party Certification Authorities
- Supports Self Certification

Seamlessly works with:

- Netscape Navigator 2 and 3
- Netscape Communicator
- Microsoft Internet Mail and Outlook Express (Internet Explorer)
- Microsoft Exchange and Outlook
- MSN (Microsoft Online Network) 2.5
- Eudora Light and Eudora Pro
- Pegasus
- Calypso
- TurnPike
- Parsons E-mail 2000
- Symantec ACT! 4

Independently reviewed by communications security experts

*RPK InvisiMail has been tested and certified by the*
International Computer Security Association

**Legend:-**

- All Versions
- Deluxe and Enterprise Editions Only

We recommend that once you have installed RPK InvisiMail, you send a FREE copy of InvisiMail Intro to everyone in your e-mail address book. This will allow your correspondents to communicate with you securely when sending and receiving e-mail. They will be able to receive and decrypt any message that you send to them. They will be able to use Strong (but not Extreme) encryption. They will not be able to compress or authenticate messages unless they upgrade to RPK InvisiMail Deluxe or Enterprise Edition. You can send the software by selecting "Send to Friends" from the RPK InvisiMail Programs menu or from the RPK InvisiMail Control Panel. You should not send to news groups as Invisimail does not use the same protocol for data transfer as news servers and it is an inappropriate way to try and distribute your key/s or InvisiMail Intro.

*Note: For those that use RPK InvisiMail in countries where export of strong encryption is restricted or regulated, please note that the RPK InvisiMail Intro Download program that you will send to others contains no encryption software.*

# Installation Screens Help

RPK InvisiMail easily guides you through the installation process.
On choosing to install, InvisiMail displays a welcome screen with a list of e-mail client's that are automatically supported by the Install process. Supported products include:-
Eudora Light, Eudora Pro, Netscape Navigator, Netscape Communicator, MSN 2.5, Calypso, Microsoft Internet Mail 3.0, Microsoft Outlook express (I.E. 4.0), Microsoft Outlook, Microsoft Exchange, Pegasus Mail, Turnpike, Parsons E-mail 2000 and Symantec ACT! 4.

If you have an alternative POP3/SMTP compliant e-mail client it is possible to manually configure InvisiMail to support your system..

Depending on your install you will now be provided with the License screen in which to input the license information provided by your sale agent. The license screen is case sensitive so be careful when entering the provided license details.

You will now be provided with the license agreement form which must be accepted to proceed with the installation. Please read this document thoroughly. You will now be prompted to close any e-mail client that may be open. We strongly recommend that you close all other open programs at this point including any web browser that you may be using.
InvisiMail will now proceed to recommend locations for storing its operational files and Data - in general we recommend that you accept the default locations.

Following this InvisiMail will search your machine for installed e-mail clients with which it can integrate; this may take some time. When InvisiMail has completed its search it will provide a list of all mail clients found on your machine. Please note InvisiMail may find ghost installs from previously installed e-mail accounts that haven't been removed completely during the uninstall process. This is of no concern, simply click to remove the tick boxes against those mail clients you do not wish to protect. When you have made your selection click the Next button.

InvisiMail now asks that a security level be selected. Please note that 607 bit encryption is more than adequate for most purposes and that choosing 1279 bit encryption may cause noticeable delays during the send and receive process. It is also important to note that the key size you select is the level of security at which others will encrypt messages to you not vice versa. As such, consideration should be given for those with whom you wish to communicate as these are the people who will experience the encryption delays. Now simply click in the appropriate security level radio box you desire and choose next.

InvisiMail requires a good source of random data to generate your Public/Private key sets which is provided by scribbling with the mouse in the view pane presented. Once InvisiMail has collected sufficient random data you will be informed and advised to click next.
InvisiMail will now ask that a default e-mail address be selected from the list identified during the earlier search for e-mail clients – it is possible to add an address at that stage if you wish.
Please note, the default address is the address which your public/private key set will be associated with on your and other machines. The other e-mail addresses will be aliases to the same key. I.e. if you have an address for your local network mail server such as steve@company.mail and an address with which you communicate with the rest of the world such as steve@somewhere.com the somewhere.com address is likely to be a good candidate for the primary address.

InvisiMail will request that a password be provided. This password will be used whenever you log on to your machine or attempt to send e-mail so DO NOT FORGET IT and be aware that the password is case sensitive. If you forget your password you will not be able to send or receive encrypted mail, it will also be impossible to read messages that you may have encrypted in your in-box.

You will now be presented with a ports screen that shows the default ports used for POP (incoming) and SMTP (outgoing) mail. Some applications such as Wingate or MimeSweeper use these ports for their own purposes and as such alternatives such as 3110 and 3025 should be used. IMAP4 is not supported in this version of InvisiMail. Now click Next.
InvisiMail has finished gathering all the information required to install on your PC and provides an overview of the information it has collected for the proposed install. Please check that this is correct before choosing Next. You will also be asked to log into InvisiMail while it encrypts your public/private key information and generates its secure data files.

Next you will be prompted to send InvisiMail to friends. This notifies correspondents that have InvisiMail of your public key so that they can send secure messages to you. For correspondents who do not have InvisiMail the notification also sends a downloader program. The downloader program enables the recipient to download Invisimail so you can begin communicating securely. Please note the downloader provide the free InvisiMail Intro version. Your correspondents may choose to upgrade to the Deluxe version to gain the additional features of compression, authentication and anti-virus integration. It is possible to personalise the "send to friends" message to suit your requirements. Please be careful not to include newsgroups in your distribution list.

InvisiMail will now asks if you would like free notification of updates and new releases. We strongly recommend you select Yes so you will be able to benefit from product enhancements as they become available.

Finally you will be asked to select the appropriate option that best describes your connection to your mail server: through dial-up modem to your Internet Service Provider or LAN based to your network mail server. This information is used to optimise the performance of InvisiMail to suite your configuration.

## Testing the installation

After running the InvisiMail installer it is a good idea to send a test message to yourself to see that InvisiMail has correctly configured your e-mail clients. You should see the InvisiMail progress display as the message is being encrypted and sent. On retrieval of the message you should again see the InvisiMail progress display and if you have a Deluxe or Enterprise Edition there will also be a File Signature.rpk attachment. The File Signature attachment contain information as to the sender of the message/that it was received encrypted and that no change was made to the file during transit.
If you receive a message such as mail server unobtainable it is likely that InvisiMail has been unsuccessful in amending your e-mail settings which will now need to be set manually. Please see trouble shooting your installation.

# Troubleshooting installation

The most common error that will be received is likely to be server unobtainable or no InvisiMail progress display during send and receive. Typically this will occur if Invisi.exe has been unsuccessful at loading in the background. Be sure to check that the InvisiMail icon is loaded in the tray on the bottom right of the screen, if not choose to run Invisi.exe from the InvisiMail Business Directory.

If Invisi.exe is running but you still receive a Server unobtainable error it is likely that InvisiMail has been unsuccessful at amending your e-mail client setting to route via InvisiMail. a likely cause is that the e-mail client/browser was not closed during the installation process which would lock the addressing files so that the amendment couldn't be made.

To correct this setting CLOSE YOUR E-MAIL OR BROWSER  then open the InvisiMail Manager and click on the Software Button. The left hand view pane details the clients that have been identified during the install. If no clients are shown, or if one is missing, choose Update E-mail. Otherwise select the e-mail client that you wish to amend by clicking in the action box. In the right hand pane the original settings should be displayed for the e-mail client along with the local address which InvisiMail is now routing communications through (e.g. 127.0.2.1). Choose to Stop InvisiMail protecting this client then close the Manager.

Now Open your mail package and check that your SMTP/POP3 settings are correct for you internet service provider or network mail server and amend as necessary. Now close the e-mail client/browser and open the InvisiMail Manager and click on the Software Button. In the left hand view pane click on the "Update e-mail software" button. InvisiMail will then search your computer for your e-mail settings, when this has been completed click and select the e-mail client in the left hand pane you are amending. In the right hand pane the correct setting should now be shown – click on the Start InvisiMail protecting button and note the modified communication settings. Now close the InvisiMail Manager and open your e-mail client and attempt to send an e-mail message to yourself. InvisiMail should then display the encryption /decryption progress screen as the message is sent.

If the progress display does not appear, be sure to check the SMTP/POP3 setting in the e-mail client which should be the amended settings (127.0.0.x) noted from the InvisiMail Manager – If different, enter the setting shown in the InvisiMail Manager.

# Planning your Network Server installation

## System requirements:-

**For Windows 95**
InvisiMail Business Edition Server for Windows 95
8MB Free Memory (Heavy loads will increase the memory requirement)
6MB Free Hard Disk Space
Windows Compatible PC
Network Configuration: Minimum Processor Pentium 166

**For Windows NT**
InvisiMail Business Edition Server for Windows NT
16MB Free Memory (Heavy loads will increase the memory requirement)
9MB Free Hard Disk Space
Windows NT Compatible PC
Network Configuration: Minimum Processor Pentium 166

InvisiMail Business Edition Server (IBES) can be configured to perform 4 separate functions:
1. External SMTP Gateway
2. External Network Server Link
3. Internal Network Server
4. Distributed Network

Each IBES solution provides the Network Administrator with different options over where information is in plain text and where it is encrypted. For the purposes of the IBES install information is categorised as follows:

- In Public in the Public Domain and generally refers to messages in the Internet
- External between your company e-mail system and the public domain.
- On Server stored on your e-mail server
- Internal between your e-mail server and an user
- Client on a user's machine.

These categories can be related to equipment with in your network e.g.

| | |
|---|---|
| Internet Router | In Public |
| FireWall | External |
| Mail Server | On Server |
| Company Network | Internal |
| Your Workstation | Client |

On an SMTP/POP3 based mail network the IBES can be installed at any location between the In Public and Client Categories. For other e-mail systems such as MS Exchange Server, Lotus Notes and Group Wise the IBES must be installed at the External Level.

**IBES External Network Server Link**
IBES is installed between any External Devices and the E-mail Server.
**Note** products that perform Virus or Content scanning must be located between IBES and e-mail server.

| **Network Device** | | **Category** | **Encrypted/Plain Text** |
|---|---|---|---|
| Internet Router | - | In Public | Encrypted |
| FireWall | - | External | Encrypted |
| **IBES Network Server Link** | | | |
| Virus Scanner | - | External | Plain Text |

| | | | |
|---|---|---|---|
| Mail Server | - | On Server | Plain Text |
| Company Network | - | Internal | Plain Text |
| Your Workstation | - | Client | Plain Text |

The Network Server Link configuration is similar to the Gateway operation accept that SMTP connections are supported for sending of messages only and POP3 is used to retrieve incoming Messages. This configuration should be used when only protection of Public Domain messages is required and mail is collected from a network service provider or POP3 Mail Server.

**IBES Internal Network Server**
IBES is installed between the Mail Server and the Network Users. You internal network must be re-configured to use InvisiMail as the Network Mail Server. For example if your computers on your network currently reference Mail.MyCompany.Com as its mail server then Mail.MyCompany.Com should be changed to point at the InvisiMail Server or each workstation should be changed to use Invisi.MyCompany.Com (please note you will need to configure this address in your DNS). The IBES Network Server may be installed on the same machine as your mail server providing the mail server software supports either TCP/IP Port Mapping or can be bound to a specific IP Address.

| **Network Device** | | **Category** | **Encrypted/Plain Text** |
|---|---|---|---|
| Internet Router | - | In Public | Encrypted |
| FireWall | - | External | Encrypted |
| Virus Scanner | - | External | Encrypted |
| Mail Server | - | On Server | Encrypted |

**IBES** Network Server

| | | | |
|---|---|---|---|
| Company Network | - | Internal | Plain Text |
| Your Workstation | - | Client | Plain Text |

The Network Server configuration protects information while it is held on your e-mail server. Network Users connect to the Email Server via the IBES Network Server which encrypts/decrypts messages as appropriate. In addition to supporting SMTP/POP3 mail servers this configuration also supports e-mail proxy servers such as WinGate.
VIRUS WARNING: ANY VIRUS SCANNING SOFTWARE NOT ON YOUR CLIENT WORKSTATIONS WILL NOT DETECT VIRUSES IN ENCRYPTED MESSAGES.

**IBES Distributed Network**
IBES Data Files are stored on a central file server, InvisiMail Workstation software is loaded on to each PC.

| **Network Device** | | **Category** | **Encrypted/Plain Text** |
|---|---|---|---|
| Internet Router | - | In Public | Encrypted |
| FireWall | - | External | Encrypted |
| Virus Scanner | - | External | Encrypted |
| Mail Server | - | On Server | Encrypted |

**IBES Data Files on a File Server**

| | | | |
|---|---|---|---|
| Company Network | - | Internal | Encrypted |

**InvisiMail Workstation Software**

| | | | |
|---|---|---|---|
| Your Workstation | - | Client | Plain Text |

This offers the highest level of security, protecting messages to and from the Workstation. This configuration also supports shared recipient lists, public and private keys.
VIRUS WARNING: ANY VIRUS SCANNING SOFTWARE NOT ON YOUR CLIENT WORKSTATIONS WILL NOT DETECT VIRUSES IN ENCRYPTED MESSAGES.

**IBES Other Configurations**
The InvisiMail Business Edition Server provides a flexible network configuration. The above represents the main options but it is possible to create hybrid configuration to suit most requirements.

In seeking to integrate with the plethora of e-mail solutions currently available and supporting future releases of such software essentially rules out any solution that attempts to use an API approach. The simple fact is that all Internet e-mail packages support Internet Protocols making the communication protocol the ideal place from which to provide security. InvisiMail achieves this by utilising local proxy techniques that convince the existing Mail Client or Server that InvisiMail is the Mail server/Internet Connection while InvisiMail in turn points out to the real service. By capturing this traffic, all e-mail passes through the InvisiMail local proxy where upon it is automatically and intelligently encrypted/decrypted passed through or seeded/scanned with/for public key data. This process allows InvisiMail to integrate with a wide range of e-mail servers including Lotus Notes, Novell GroupWise, MS Exchange and a number of complimentary content security solutions.

The Connection display in the InvisiMail Manager displays the IP address on which InvisiMail will accept communications from the Local Network for routing mail. In so doing it provides the ability to support multiple Mail Servers in a distributed network or in a network installation with centralised encryption it will accept connections from listed clients. Within this section is the ability to set the IP profile from the "Allowed List" button and specifically deny external Internet Connections.

## Management Tasks and Considerations

**Tasks to Install External Network Server Link**
1. Note the IP Address and SMTP/POP3 Ports (Usually 25 and 110) of the External Mail Server to where external Email Messages are sent and from where Internal Messages may be retrieved.
2. Note the IP Address and SMTP/POP3 Ports (Usually 25 and 110) of the InvisiMail Server.
3. Prepare a list of the Users and email addresses (see below for File Format to enable import during Install)
4. Ensure you have an InvisiMail Network license to cover the number of users/keys required.
5. Install InvisiMail Network Server for Windows NT or Windows 95 as required.
6. Alter the send and retrieve addresses of your email server to ensure that mail is routed via the InvisiMail Server.
7. By Default InvisiMail accepts all connections. Use the Connections Screen in the InvisiMail manager to DENY access to the server as required.

**Tasks to Install Internal Network Server**
1. Note the IP Address and SMTP/POP3 Ports (Usually 25 and 110) of your Network Mail Server.
2. Note the IP Address and SMTP/POP3 Ports (Usually 25 and 110) of the InvisiMail Server.
3. Prepare a list of the Users and email addresses (see below for File Format to enable import during Install)
4. Ensure you have an InvisiMail Network license to cover the number of users/keys required.
5. Install InvisiMail Network Server for Windows NT or Windows 95 as required.
6. Alter the send and retrieve addresses of your email workstations or your internal DNS server to ensure that mail is routed via the InvisiMail Server.
7. By Default InvisiMail accepts all connections. Use the Connections Screen in the InvisiMail manager to DENY access to the server as required.

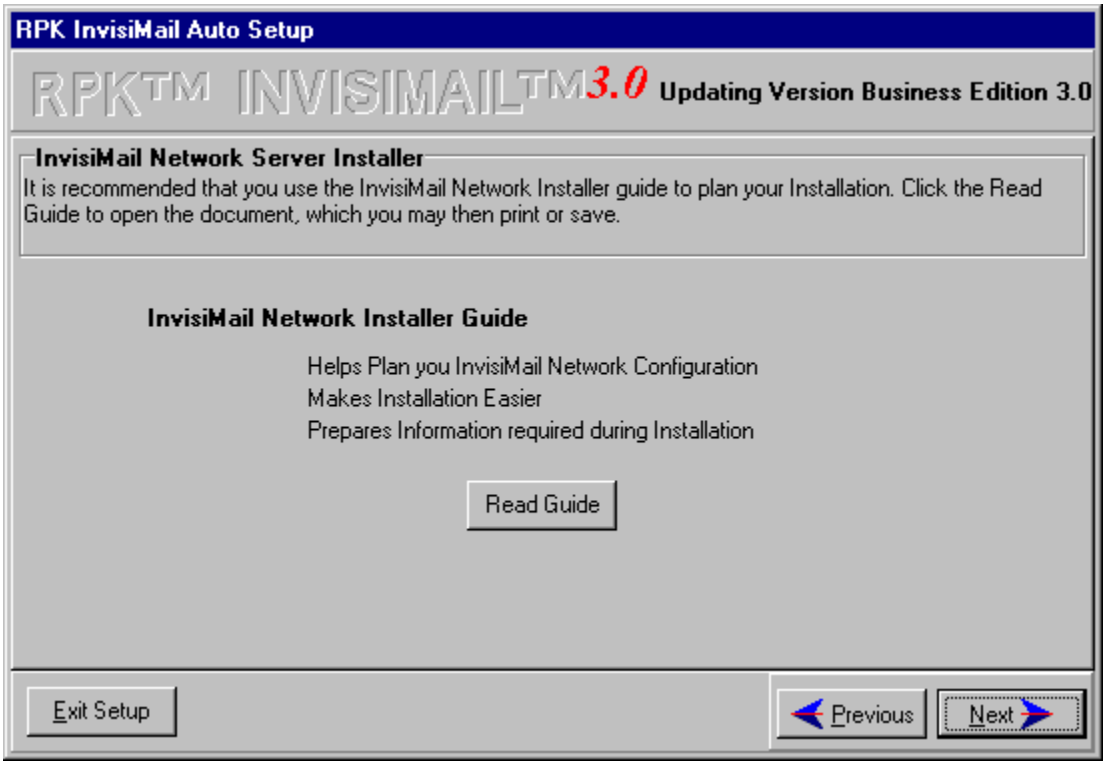
Virus Scanning and Content Filtering: It is important to note that encrypted data cannot be checked for viruses or content. This must be considered when designing your Installation. Ensure that you take adequate steps to support these vital tasks. See the InvisiMail Web Site for more information on Encryption and Virus Scanning.

Data Backup: Remember to include the InvisiMail Data Directory in your Network Backup policy. Information such as Private Keys and Authentication Data cannot be recreated if lost.

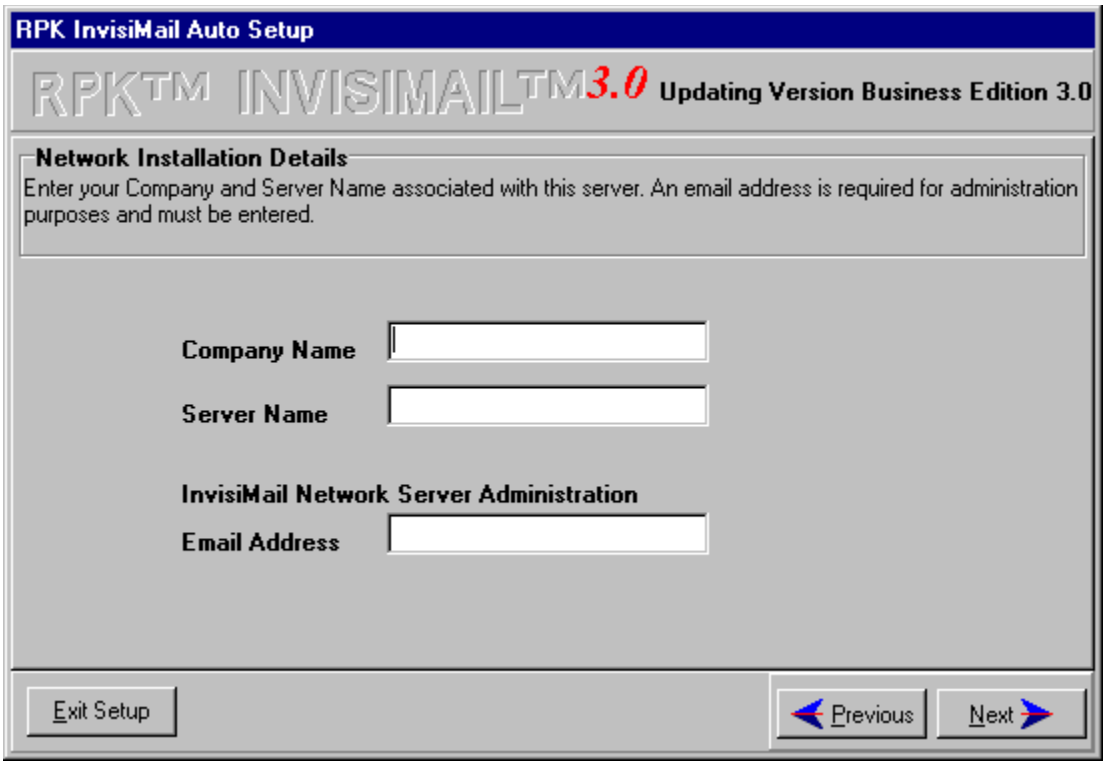
## Installation screens

After launching the installer and clicking Setup you will be greeted with a splash screen telling you which version of InvisiMail you are installing. The following screen (below) asks you to read the **Installer guide** (strongly recommended) before proceeding; this guide information is also available in the Planning installation section of these help files.

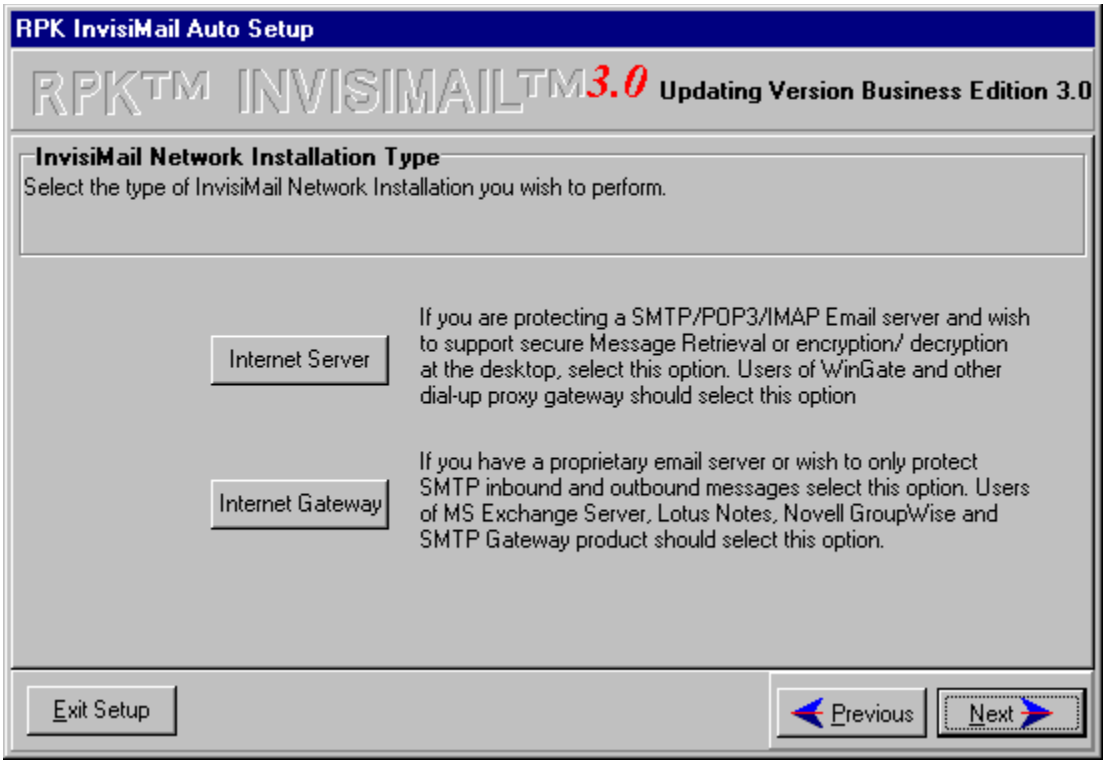
*The information you are asked to gather by the guide is necessary for your installation of InvisiMail to function correctly.*



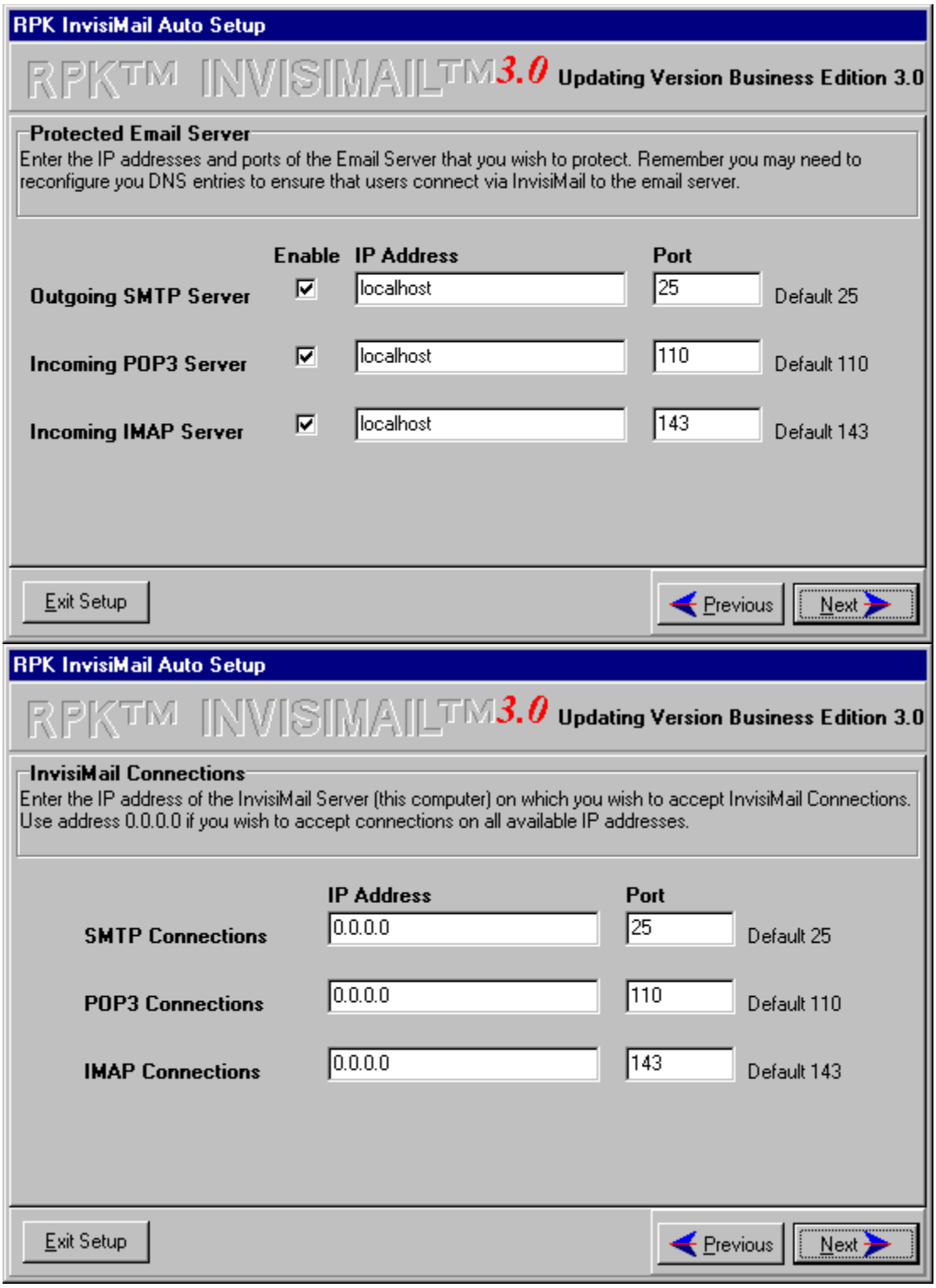

You must enter a company name, server name and an e-mail address before you are allowed to progress with the installation.




Pick the type of network install that suits the network configuration you are using. If you are in doubt as to which option you should choose, ask your Systems Administrator or contact InvisiMail Technical Support for assistance.



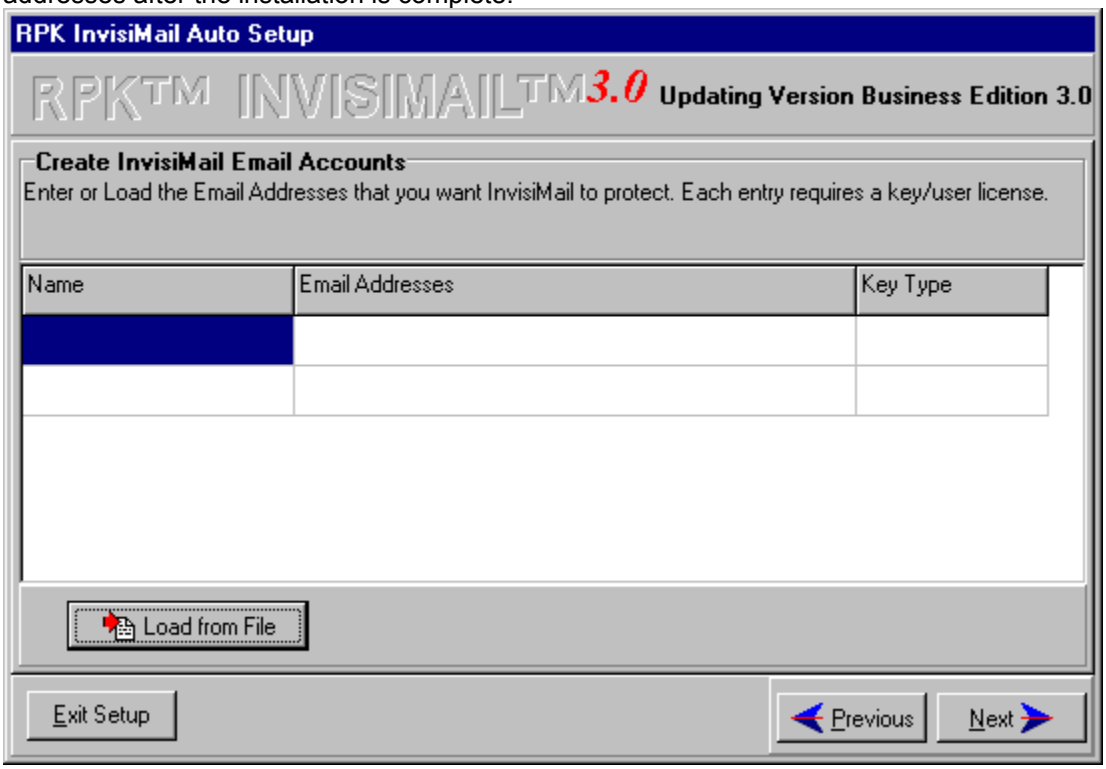

The next screen that appears will depend on which of the above options you chose. Firstly, we will deal with the Internet Server option (please scroll down if you wish to see the Internet Gateway screens).




After this screen you will be asked to enter any e-mail addresses you wish to use. It allows you to import a pre-defined list of e-mail addresses into InvisiMail's address book. This should be done in advance by setting up a text file with users names and e-mail addresses in the following format:
The columns of data are separated by a tab. E-mail addresses are separated by a comma.

John Smith	Jsmith@MyCompany.Com,John_Smith@MyCompany.co.uk
Bill Brown	BBrown@MyCompany.Com,Bill_Brown@MyCompany.co.uk
MyCompany	*@MyCompany.Com

UKBranch *@MyCompany.Co.uk
By clicking on the Load from File button you will be able to pick the location of your prepared file and then upload it into InvisiMail's address book. You can, of course, type in your addresses or add further addresses after the installation is complete.




The installation continues with the selection of the directories you wish to use and the default key strength that you require.
*If, however, you previously selected the Internet Gateway option then the e-mail address screen will be presented to you first, followed by the two screens below.*

## Network Server License

Licensing is based on cost per seat i.e. you must purchase a license sufficient to cover all users, not just for one machine (the Network Server). If you do not have a valid license number to enter during installation, then a time-limited two user version will be all that is available.

You may upgrade a license after installation on the license page in InvisiMail Manager provided, of course, you have made the necessary licensing purchase.

Network Server licensing allows only one key per e-mail address, but you may have many addresses.

## Shared Data files

The Network Server edition of InvisiMail uses the concept of shared keys to provide secure communication for multiple users. If your installation of InvisiMail is encrypted to the desktop i.e. you have InvisiMail on your PC to decrypt your messages on receipt rather than have a server do it for you, then it will be possible for you to have shared data.
This concept allows you to have a shared private key and a personal private key thus enabling others to use the shared key without compromising the security of your private files. Any shared keys that you create on the Private keys page within InvisiMail Manager can be viewed by clicking on the Public keys button at the bottom of the Private keys page.

## Private Data files

Private data files are those which you secure with your private key and must log on to InvisiMail Manager to access (this process is normally performed on startup). When using the Network Server edition this is only possible if you have encryption to your desktop, which is where your private files would be stored. Otherwise your files would be handled by the Server and arrive at your PC already decrypted.

## Testing the Network install

After running the InvisiMail installer it is a good idea to send a test message to yourself to see that InvisiMail has been correctly configured. If you have encryption to your desktop, you should see the InvisiMail progress display as the message is being encrypted and sent. On retrieval of the message you should again see the InvisiMail progress display and if you have a Deluxe or Enterprise Edition there will also be a File Signature.rpk attachment. The File Signature attachments contain information as to the sender of the message, that it was received encrypted and that no change was made to the file during transit.

If you receive a message such as mail server unobtainable it is likely that InvisiMail has been unsuccessful in amending your e-mail settings which will now need to be set manually. Please see trouble shooting your installation.

If you do not have encryption to your desktop then you will not see the usual InvisiMail progress display as the message is being encrypted and sent. What you must do is to log on to the InvisiMail Network Manager, then you can look on the Trust Data page to see that your key is being recognised correctly. If you check the Private Keys page for your Key ID you can look at the Trust Data page after you have sent and received a mail to yourself; your Key ID should appear in both the Sender Key and Receiver Key reference columns.

# Planning your Gateway Server installation

## System requirements:-

**For Windows 95**
InvisiMail Business Edition Server for Windows 95
8MB Free Memory (Heavy loads will increase the memory requirement)
6MB Free Hard Disk Space
Windows Compatible PC
Gateway Configuration: Minimum Processor Pentium 100

**For Windows NT**
InvisiMail Business Edition Server for Windows NT
16MB Free Memory (Heavy loads will increase the memory requirement)
9MB Free Hard Disk Space
Windows NT Compatible PC
Gateway Configuration: Minimum Processor Pentium 100

InvisiMail Business Edition Server (IBES) can be configured to perform 4 separate functions:

1. External SMTP Gateway
2. External Network Server Link
3. Internal Network Server
4. Distributed Network

Each IBES solution provides the Network Administrator with different options over where information is in plain text and where it is encrypted. For the purposes of the IBES install information is categorised as follows:

- In Public in the Public Domain and generally refers to messages in the Internet
- External between your company e-mail system and the public domain.
- On Server stored on your e-mail server
- Internal between your e-mail server and an user
- Client on a user's machine.

These categories can be related to equipment with in your network e.g.

| | |
|---|---|
| Internet Router | In Public |
| FireWall | External |
| Mail Server | On Server |
| Company Network | Internal |
| Your Workstation | Client |

On an SMTP/POP3 based mail network the IBES can be installed at any location between the In Public and Client Categories. For other e-mail systems such as MS Exchange Server, Lotus Notes and Group Wise the IBES must be installed at the External Level.

**IBES External SMTP Gateway Option**
IBES is installed between any External Devices and the E-mail Server.
**Note** products that perform Virus or Content scanning must be located between IBES and e-mail server.

| Network Device | | Category | Encrypted/Plain Text |
|---|---|---|---|
| Internet Router | - | In Public | Encrypted |
| FireWall | - | External | Encrypted |
| **IEBS Gateway** | | | |
| Virus Scanner | - | External | Plain Text |
| Mail Server | - | On Server | Plain Text |
| Company Network | - | Internal | Plain Text |
| Your Workstation | - | Client | Plain Text |

The IBES Gateway will accept INBOUND connections from the Firewall and OUTBOUND connections from the Virus Scanner. INBOUND connections MAY ONLY BE DECRYPTED, Out Bound connections MAY ONLY BE ENCRYPTED. The Gateway configuration supports SMTP connections only.

**Installing an External SMTP Gateway**

To install the InvisiMail Gateway it is necessary have a basic understanding of TCP/IP and Networking issues. As part of the install process the administrator is directed to read the Network Installer Guide which contains much of the information held in this document. To assist in the install process InvisiMail provides a wizard based install that guides the Network Administrator through the installation process advising as to the appropriate settings for the mail server and Firewall.

1. Note the IP Address and SMTP Port (Usually 25) of the Server from which Messages will be sent to InvisiMail prior to being forward to the Internet. This may be you E-mail Server or Virus Scanner. IT WILL ALWAYS BE A SERVER OR DEVICE ON YOUR NETWORK.
2. Note the IP Address and SMTP Port (Usually 25) of the Server to which Messages will be sent. This will generally be your Internet Provider SMTP server and Relay Server. If you do not use an SMTP Server or Relay Server then visit the InvisiMail Web Site for a list of third party SMTP Relay products.
3. Note the IP Address and SMTP Port (Usually 25) of the InvisiMail Server.

The IP addressing details will be used on an installation screen where InvisiMail will determine the appropriate addresses to be used as follows:

1. On completion of your Gateway install it will be necessary to alter the forwarding address of your e-mail server/virus scanner to ensure that e-mail is forwarded to the InvisiMail Server. As this information is used the new addressing should be noted.
2. It will also be necessary to alter the forwarding address of your external systems to ensure that Inbound e-mail is routed via InvisiMail.

In seeking to integrate with the plethora of e-mail solutions currently available and supporting future releases of such software essentially rules out any solution that attempts to use an API approach. The simple fact is that all Internet e-mail packages support Internet Protocols making the communication protocol the ideal place from which to provide security. InvisiMail achieves this by utilising local proxy techniques that convince the existing Mail Client or Server that InvisiMail is the Mail server/Internet Connection while InvisiMail in turn points out to the real service. By capturing this traffic, all e-mail passes through the InvisiMail local proxy where upon it is automatically and intelligently encrypted/decrypted passed through or seeded/scanned with/for public key data. This process allows InvisiMail to integrate with a wide range of e-mail servers including Lotus Notes, Novell GroupWise, MS Exchange and a number of complimentary content security solutions.

The Connection display in the InvisiMail Manager displays the IP address on which InvisiMail will accept communications from the Local Network for routing mail. In so doing it provides the ability to support multiple Mail Servers in a distributed network or in a network installation with centralised encryption it will accept connections from listed clients. Within this section is the ability to set the IP profile from the "Allowed List" button and specifically deny external Internet Connections.

## Management Tasks and Considerations

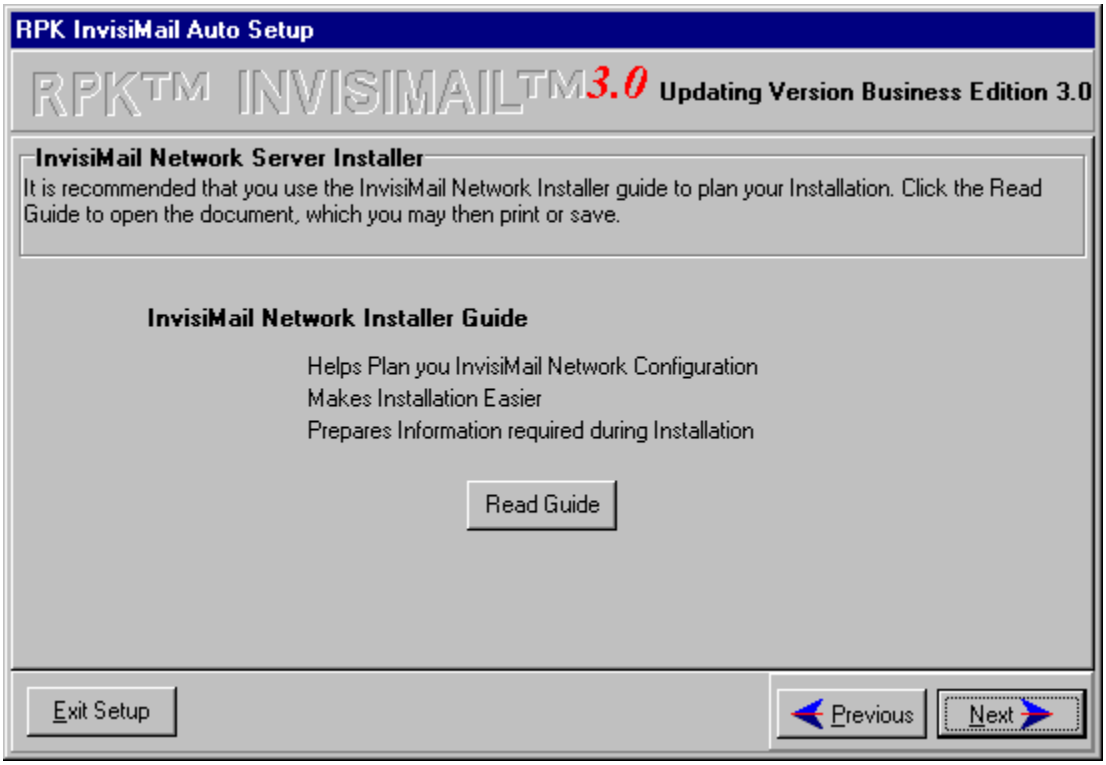
Virus Scanning and Content Filtering: It is important to note that encrypted data cannot be checked for viruses or content. This must be considered when designing your Installation. Ensure that you take adequate steps to support these vital tasks. See the InvisiMail Web Site for more information on Encryption and Virus Scanning.

Data Backup: Remember to include the InvisiMail Data Directory in your Network Backup policy. Information such as Private Keys and Authentication Data cannot be recreated if lost.

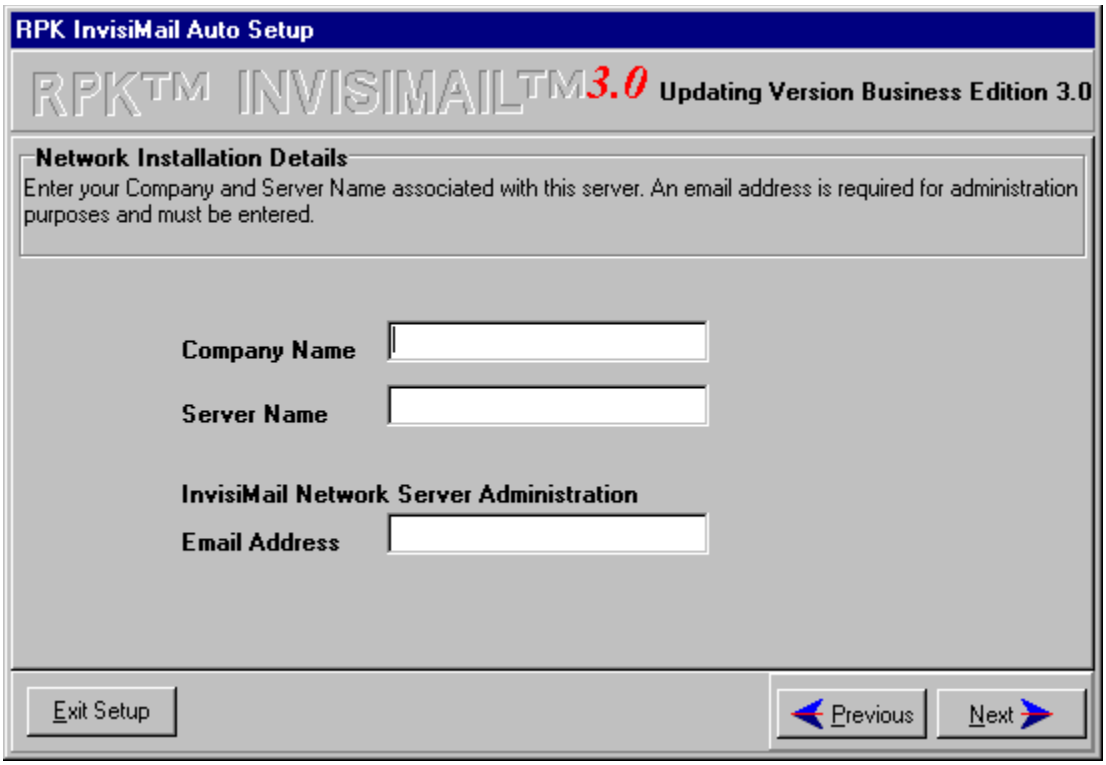
## Installation screens

After launching the installer and clicking Setup you will be greeted with a splash screen telling you which version of InvisiMail you are installing. The following screen (below) asks you to read the **Installer guide** (strongly recommended) before proceeding; this guide information is also available in the Planning installation section of these help files.

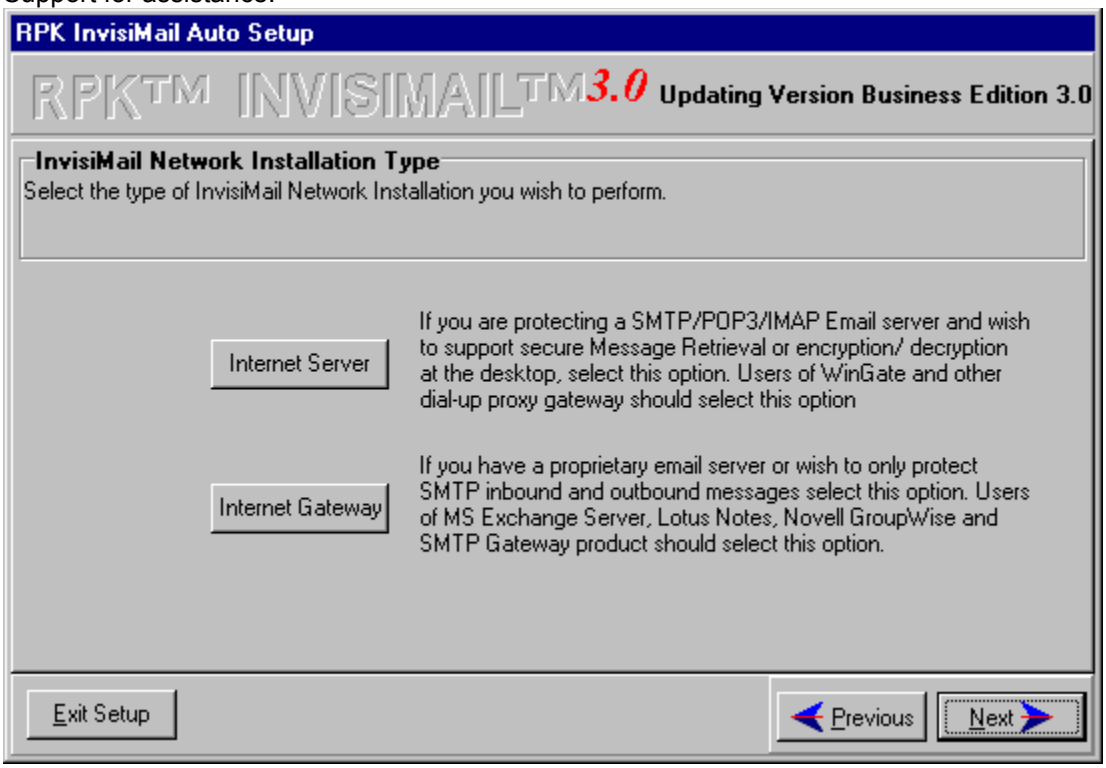
*The information you are asked to gather by the guide is necessary for your installation of InvisiMail to function correctly.*



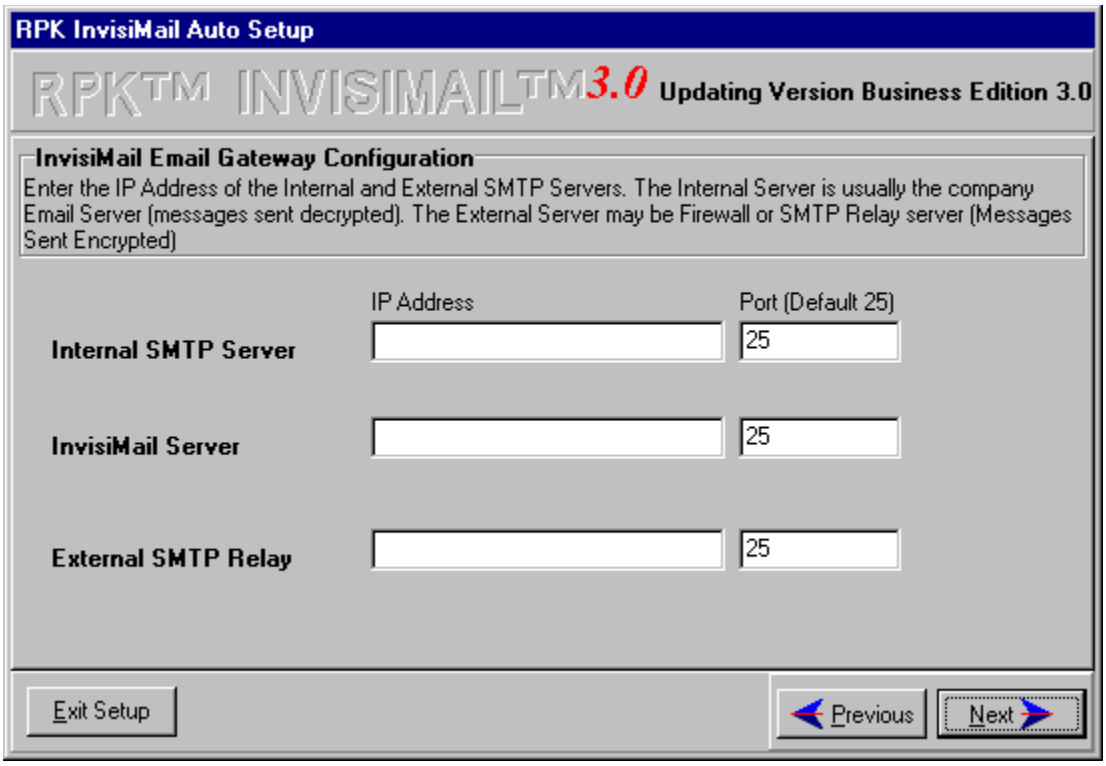

You must enter a company name, server name and an e-mail address before you are allowed to progress with the installation.

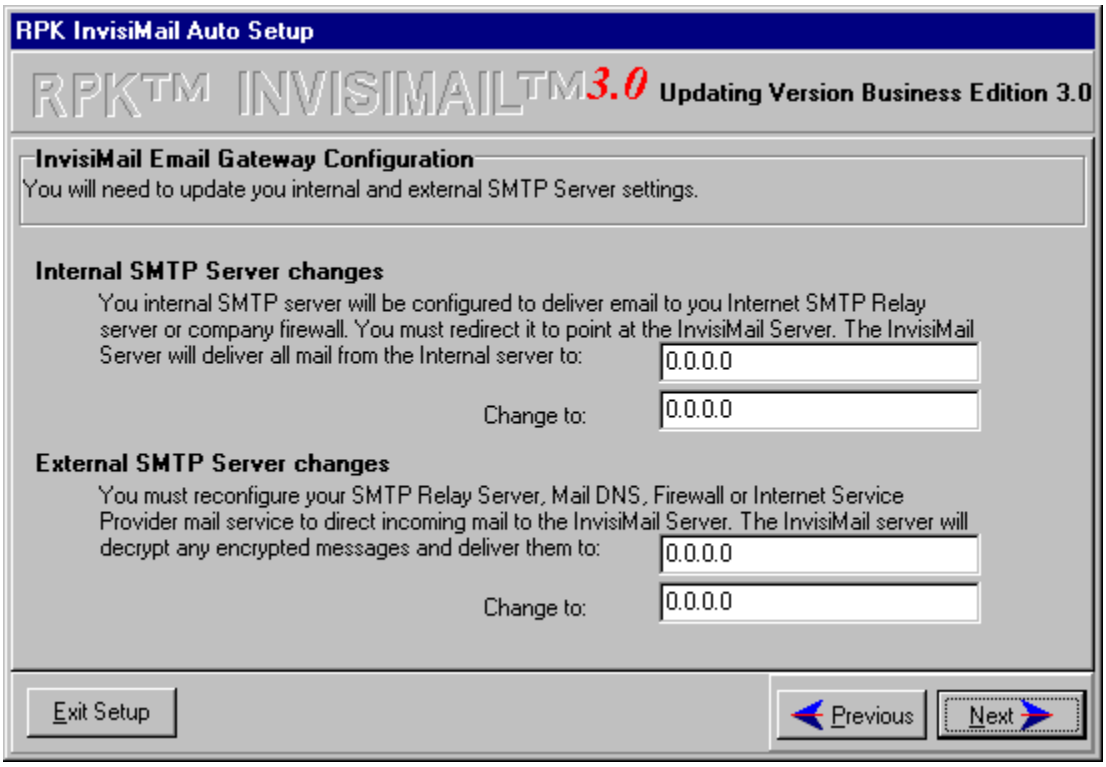



Pick the type of network install that suits the network configuration you wish to use. If you are in doubt as to which option you should choose, ask your Systems Administrator or contact InvisiMail Technical Support for assistance.




Having chosen Internet Gateway to allow the installation of the InvisiMail Gateway Edition of the product, the IP address and port information that you gathered earlier can now be entered in the appropriate boxes.




The installation will now continue as per the Internet Server option i.e. with confirmation of the directories to be used and the default key strength required.

## Gateway License

Licensing is based on cost per seat i.e. you must purchase a license sufficient to cover all users, not just for one machine (the Gateway Server). If you do not have a valid license number to enter during installation, then a time-limited two user version will be installed.

Gateway Server licensing allows users to have multiple keys assigned to e-mail aliases. IP addressing can be used to limit the users who can send mail via InvisiMail to the licensed figure allowed. This is acheived by denying access to all those except specific IP addresses or a range of IP addresses on the Allowed List, from the Connections page in InvisiMail Manager. Most Gateway installs will consist of a relatively small number of corporate e-mail addresses e.g. *@mycompany.com, sales@mycompany.com etc.

You may upgrade a license after installation on the license page in InvisiMail Manager provided, of course, you have made the necessary licensing purchase.

## Testing the Gateway install

After running the InvisiMail installer it is a good idea to send a test message to yourself to see that InvisiMail has been correctly configured. You will not see the usual InvisiMail progress display as the message is being encrypted and sent; the InvisiMail Gateway is completely invisible to the end user and there are no progress screens on the server in order to maximise processing power for network throughput.

There will be a File Signature.rpk attachment in your received mail messages that have come from another InvisiMail user/server (or from yourself). The File Signature attachments contain information as to the sender of the message, that it was received encrypted, that no change was made to the file during transit and will tell you if there is a digital signature available for the sender.

If you log on to the InvisiMail Gateway Manager then you can look on the Trust Data page to see that your key is being recognised correctly. If you check the Private Keys page for your Key ID you can look at the Trust Data page after you have sent and received a mail to yourself; your Key ID should appear in both the Sender Key and Receiver Key reference columns.

## Using InvisiMail on the same PC as WinGate

InvisiMail can capture mail heading to the Internet via WinGate. InvisiMail sits between your e-mail clients and WinGate; the clients must be pointed to the IP and port address of InvisiMail which will in turn point to the same IP address, but must be given a separate port address to gain access to WinGate: e.g.

Client > 192.168.0.1:25 > InvisiMail > 192.168.0.1:3025 > WinGate for SMTP
Client > 192.168.0.1:110 > InvisiMail > 192.168.0.1:3110 > WinGate for POP3
Client > 192.168.0.1:143 > InvisiMail > 192.168.0.1:3143 > WinGate for IMAP

Here the client and InvisiMail are pointing to the same IP address (the same PC), but are using different ports on which to communicate. This allows the e-mail client to operate exactly as it did previously, pointing to the same address/port, but all mail will pass through InvisiMail before it reaches the Internet and all received mail will be intercepted by InvisiMail before it arrives at the desktop.

The proxy settings can be entered on the Connections tab within the InvisiMail Manager; this may be done during installation if you are using the Enterprise edition or anytime after install through the Manager.

WinGate will require re-configuring to listen for e-mail traffic on the ports you have assigned in InvisiMail. This can be done within WinGate's GateKeeeper administration program. By selecting Services - POP3 and SMTP, you can change the port configuration on the General tab within the Properties page of each Service. After these alterations have been made, you should restart your InvisiMail / WinGate machine to ensure all changes are implemented correctly. A test email should then be sent to yourself to check the install.

## Using InvisiMail on the same PC as your E-mail Server

How InvisiMail interacts with your e-mail server software will depend on the type of configuration you require. InvisiMail can capture mail from within the network heading to the mail server or it can perform its functions externally to the mail server (see Gateway Edition). In both cases the important issue here concerns IP and port addressing.

If InvisiMail sits between your e-mail clients and the e-mail server then the clients can remain pointed to the IP and port address of the mail server: e.g.

Client > 192.168.0.1:25 > InvisiMail > 192.168.0.1:3025 > E-mail Server for SMTP
Client > 192.168.0.1:110 > InvisiMail > 192.168.0.1:3110 > E-mail Server for POP3
Client > 192.168.0.1:143 > InvisiMail > 192.168.0.1:3143 > E-mail Server for IMAP

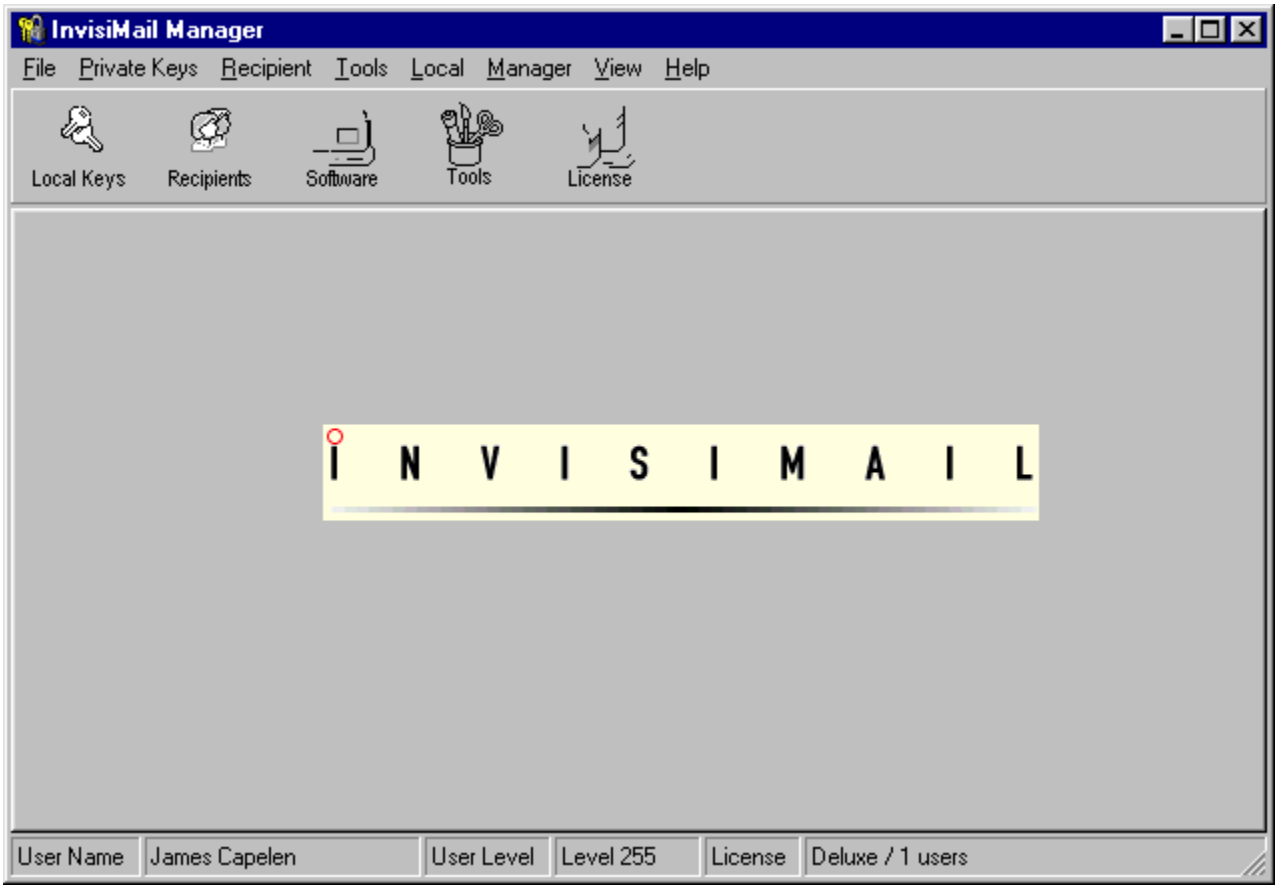
Here the client and InvisiMail are pointing to the same IP address (the same PC), but are using different ports on which to communicate. This allows the e-mail client to operate exactly as it did previously, pointing to the same address/port, but all mail will pass through InvisiMail before it reaches the Internet and all received mail will be intercepted by InvisiMail before it arrives at the desktop. The E-mail Server will require re-configuring to listen for e-mail traffic on the ports you have assigned in InvisiMail. This is usually a simple task, but certain e-mail servers e.g. Microsoft Exchange Server will require Registry settings to be altered - if in doubt speak to your Systems Administrator or contact Technical Support.

## Content Security

Just as InvisiMail seamlessly integrates with your email client, full support is provided for integration with Symantec's ACT! 4. This allows secure (607bit / 1279 bit) database synchronisation globally providing excellent additional functionality to this market leading product.

# InvisiMail Manager

The InvisiMail Manager access to user settings and all the functions necessary to administer your e-mail security. After you install InvisiMail, the Manager is available from the Systray by double-clicking on the lock and keys icon or via the Start menu in the Program files section (this assumes that the default folders created during install are being used).




Above you can see the initial splash screen of InvisiMail Manager. It is both menu and icon driven - most of the functions you will require are easily accessed by using the relevant icon on the tool bar. The rest of this section of the Help files will take you through each icon and its associated functions.

*The user name, licensing and product details on the initial Manager screen will vary depending on your installation and who is logged on to your program.*

# A brief explanation of Keys
## (Encryption and Decryption)

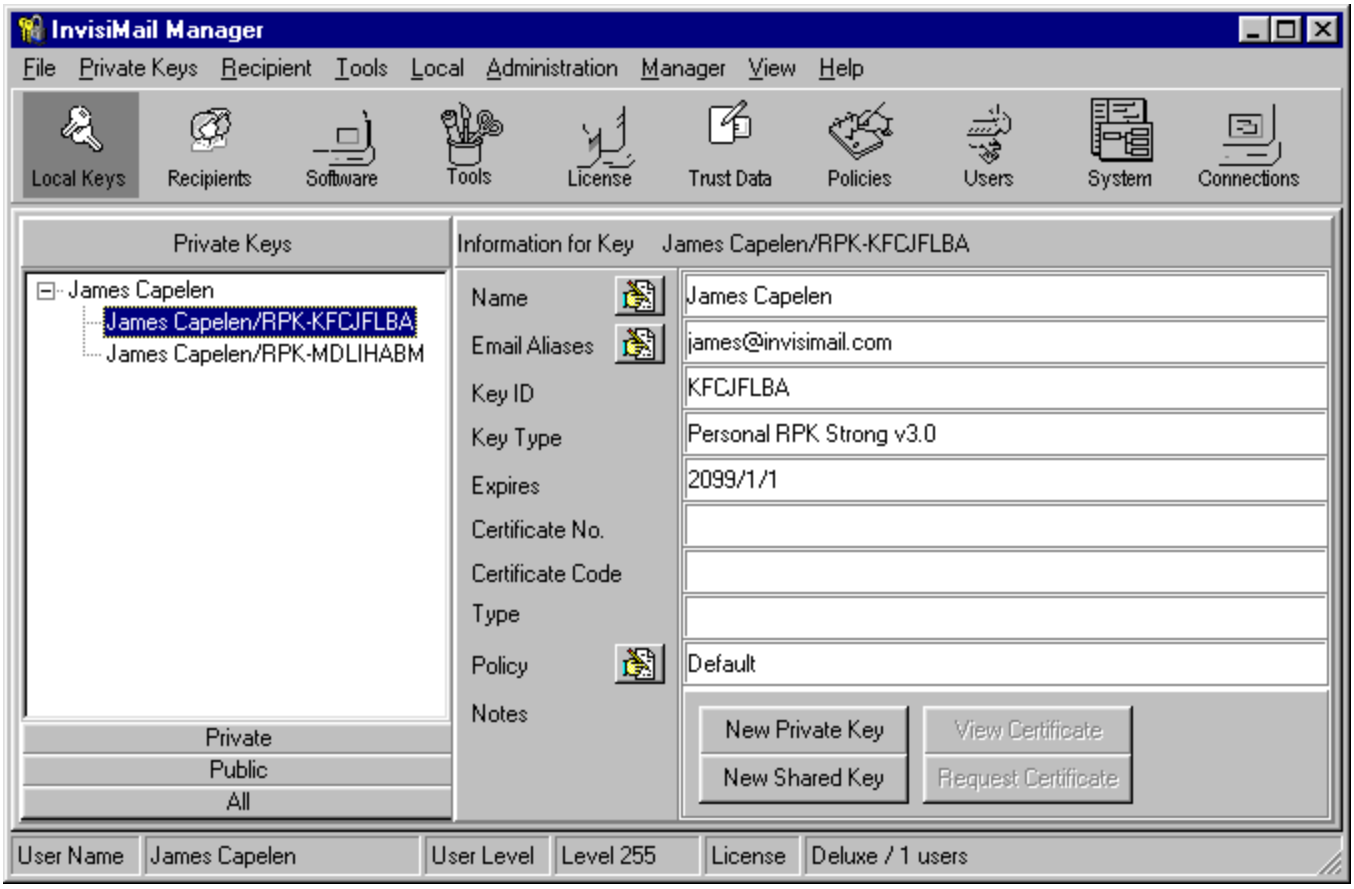
The means by which information is secured is called encryption. Decryption is the process of restoring information to its original format. The information about the underlying technology used in RPK InvisiMail is here for informational and educational purposes only. The good news with RPK InvisiMail is that you do not need to learn this material to be able to use the product.

The way in which RPK InvisiMail deals with encryption and decryption is simple in principle. Unlike doors with deadbolt locks where only one key is used to lock and unlock the door, RPK InvisiMail there are two related keys. One is used to encrypt (lock) the message, and the other to decrypt (unlock) the message. The one used to encrypt is known as the "Public Key" since it is the one that is made known publicly and used by others to encrypt messages being sent to you. This is also where the technology gets its common name "Public Key Encryption." The second key, which is used to decrypt messages sent to you, is called the "Private Key." It is called "private" because it is known only by you. RPK InvisiMail keeps track of keys for you. All you need to do is remember your RPK InvisiMail password and keep it to yourself.

With RPK InvisiMail, whenever you send a message to someone else who is using any version of RPK InvisiMail (Intro, Deluxe or Enterprise), the message will automatically be encrypted prior to sending, using the *public key* of the recipient. When that person receives the message, RPK InvisiMail will automatically use their *private key* to decrypt the message. You never have to worry about sending a message to someone they cannot read. If they do not have a copy of RPK InvisiMail, the program will not be able to encrypt before sending. In these cases you can easily send anyone a FREE copy of RPK InvisiMail Intro so you can send them secure messages.


## Viewing Key Information

Selecting Local Keys from the InvisiMail Manager Toolbar brings up the Keys page. On this page you can view, create and delete keys; you may also assign specific email addresses to the same key or to different keys, thus enabling you to have different security settings for separate e-mail accounts (see also Trust Data and Policies).
On the left-hand side of this page you will find a list of Key holders; at the left of each is a + sign, you may click on this to drop down a list of Key/s for each Key holder. A single click on the key or keys revealed will bring up that keys information on the right-hand side of the screen (see below).

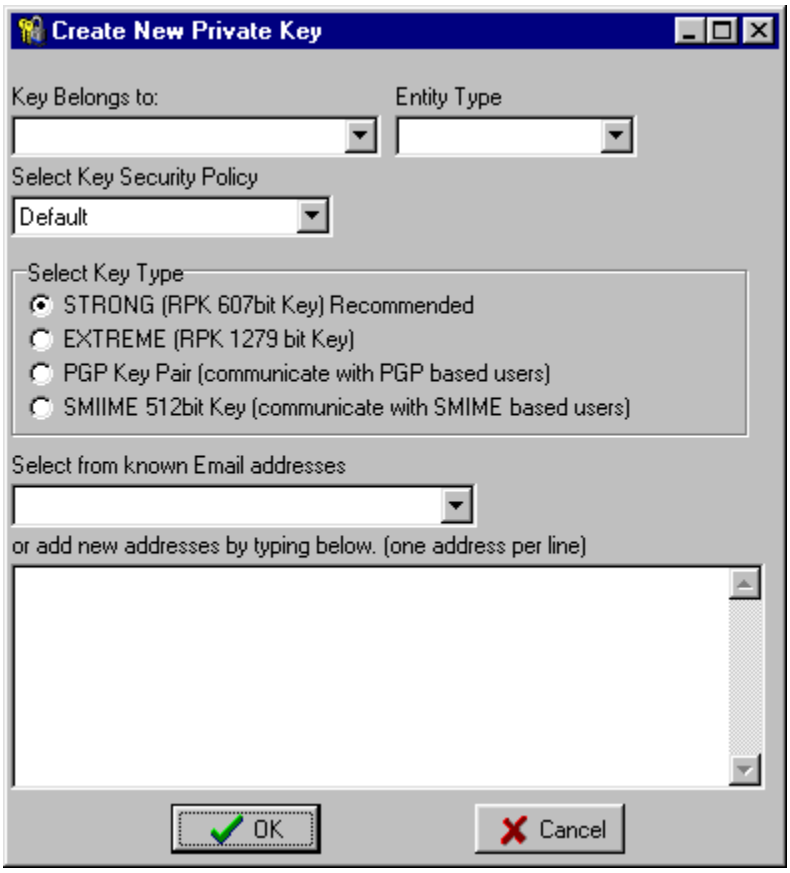



You can now see the name of the Key holder, the email address associated with that Key, the Key ID and type and its expiration date.

The buttons to the left of the Name and Email aliases can be single-clicked to bring up dialog boxes. These dialog boxes will allow you to change the name associated with this Key and to associate email aliases with this Key.

## Creating a New Key

New Keys for an existing or a new user may be created from here using the appropriate button at the bottom of this page. A dialog box is brought up, allowing the choice of Key type, Key Owner, Security Policy etc. (see below)




*The PGP Key and SMIME Key options are not available in this release of InvisiMail, but have been included to demonstrate one of the enhancements which will be available in later versions.*
You may select one or more e-mail addresses from the drop down list provided to associate with the new Key, or you may type in the address.

## Assigning E-mail Addresses to Keys

By default, the first Key you created will have been assigned an e-mail address during the installation procedure. If a user has more than one e-mail address, then more than one address can be assigned to a single key. This gives the ability to secure all your mail with one Key.

On the Local Keys page, clicking the button next to E-mail aliases will bring up a dialog box in which you may type another e-mail address to add to the list of those using that particular Key. Multiple e-mail addresses may be assigned to any key, however, ***an e-mail address*** *can* ***only*** *have* ***one Key*** *associated with it* (either 607 bit or 1279 bit).

On creation of a new Key, you may associate an e-mail address that already has a Key assigned to it, but the last assignment always becomes the default for that address.

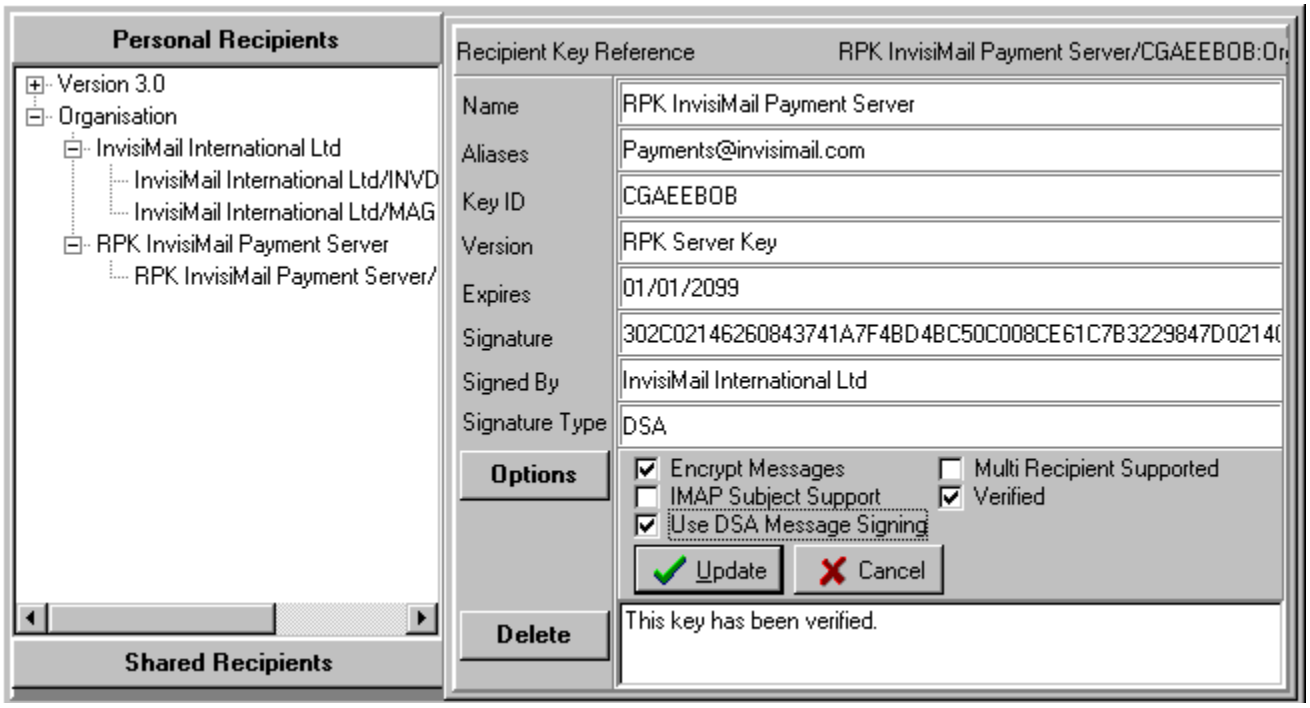
You may wish to use these options to enable Strong Encryption on one or more e-mail addresses while using Extreme Encryption on more sensitive addresses for the best possible security.

Security Policies can be assigned here using the button provided, but a policy must be setup before you can assign a new one - all keys created are given a default policy.


# Viewing Recipient Information

All users of InvisiMail with whom you communicate will appear in the Recipients list once they have sent you their Key. Their key is sent automatically in their first message to you after they install InvisiMail.

Individual Recipients and their Keys can be selected in the same way as on the Local Keys page and their information will appear on the right of the page.



## Changing options for Recipients

The following options are available for each Recipient:

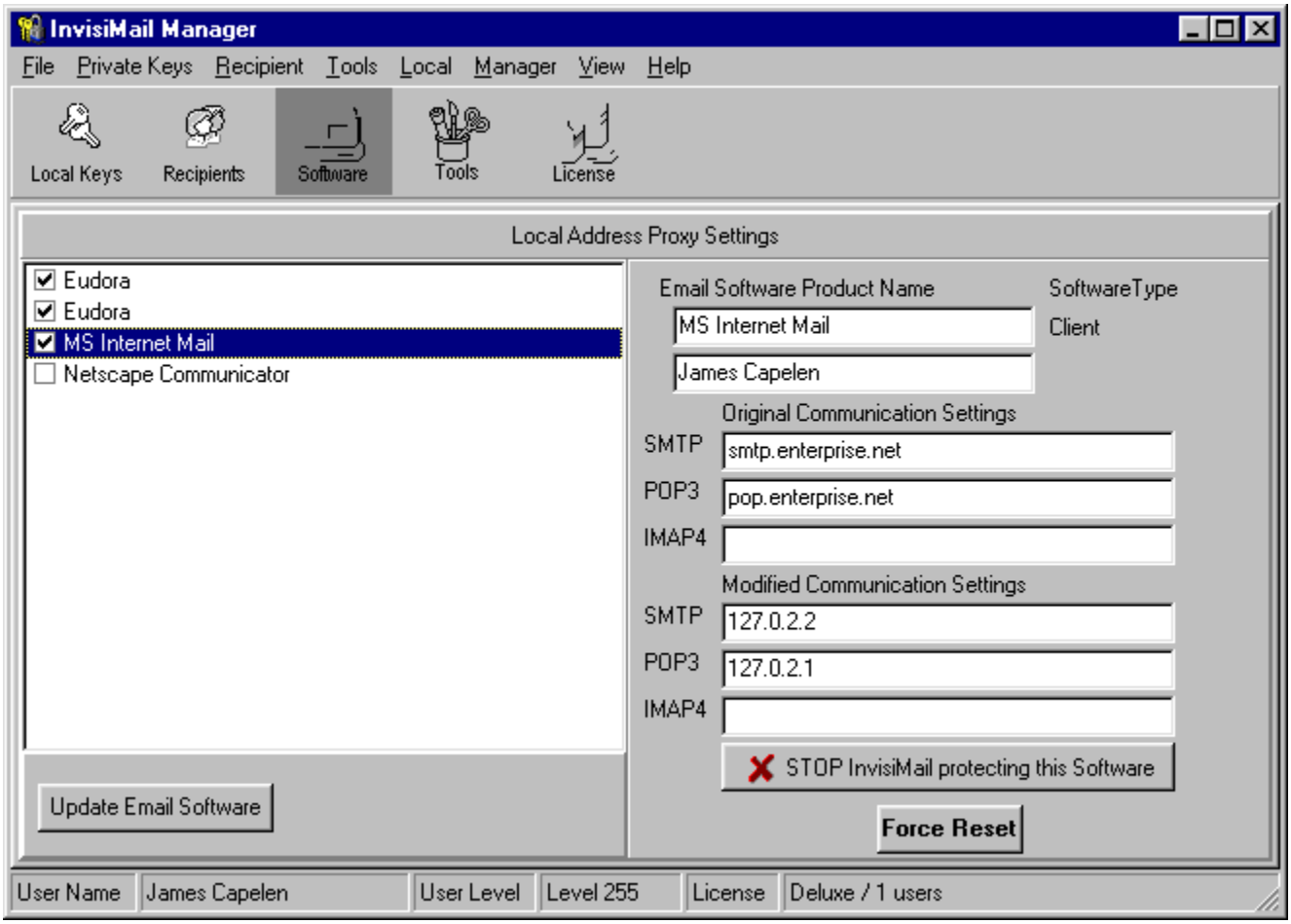
- whether to encrypt messages or not
- enable IMAP support
- use digital signatures to prevent man-in-the-middle attacks
- allow use of Multiple Recipients
- enable/disable verification


Once the required boxes have been checked/unchecked, the update button must be single-clicked to effect the changes.

Recipients may be removed from the list using the Delete button below this options panel.


# E-mail Packages

The Software page (in Deluxe/Enterprise Desktop editions only) displays all the e-mail packages detected during install. The list of compatible packages is given in the Introduction.



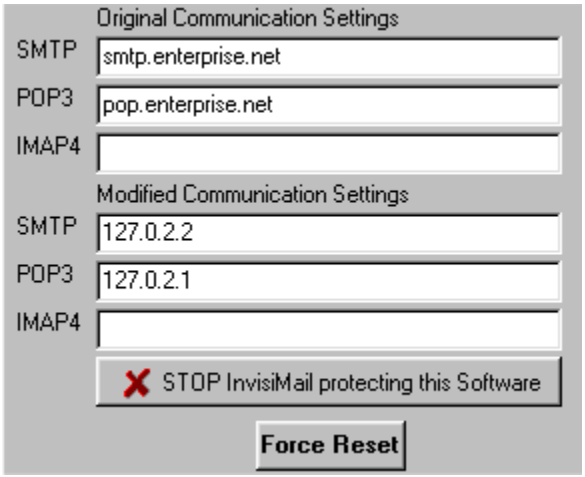

All detected Email clients are displayed in the left-hand window: the check boxes (if ticked) show that InvisiMail is currently protecting that client. There is a long button under the communication details on the right of the window which will allow you to unprotect/protect individual email clients. This would be useful for instance if one client was used for internal network mail which did not require protection and another package was used for all Internet mail and needed high levels of security.

If you do load an email program after installing InvisiMail and you wish to add the new program to the list of those already protected, use the Update E-mail Software button. Once this is complete you must select your newly detected program in the left-hand window and click on Start InvisiMail Protecting this Software on the right-hand side of the page. You should then close and re-open InvisiMail Manager to effect the changes and re-open your email software.

The Force Reset button is for use when communication on one or more of the mail ports is not performing correctly. After pressing Force Reset, you must close and then re-open your e-mail clients in order for the

changes to take effect; InvisiMail will alert you of this via a dialog box.

## Communication Settings




The original communication settings refer to the name or the address of your mail server; the modified settings are the ones being used by InvisiMail to capture your messages and encrypt/decrypt them. These settings should not need to be altered if you are using the Deluxe/Enterprise desktop edition and you are not using any other mail server-type software on your PC.


# Importing your Keys/Recipients from InvisiMail 2.1x

If you are upgrading from a version of InvisiMail 2.1x (where x is a release number), then you may attempt to import your present data into InvisiMail 3.

This process is performed on the Tools page, but should only be attempted if your previous version of Invisimail does match the version range specified. If the import fails then you will have to setup your recipients list by using the Send to Friends program in your Start Menu.

You should be aware that this option can send mail to ALL members of your Address Book if you select everybody in the list. You should not send to news groups as InvisiMail does not use the same protocol for data transfer as news servers.

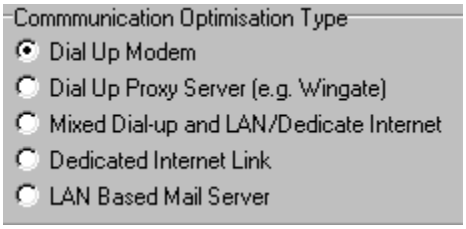
## Communications Logging

This is a built-in fault finding tool which can report all mail transactions in plain text format. It helps System Administrators/Technical Support personnel to trace problems with your mail transfers/access. See Troubleshooting installation

Logging is not turned on by default as in normal circumstances it is not required and large amounts of disk space are used to store the log.

# Communications Optimisation

On the tools page there are five options available to optimise InvisiMail for use in various network or desktop setup scenarios:-




The options provided here are to allow InvisiMail to be configured for optimal Mail server access, dependent on the method of that access. In doing so, unnecessary network or telephone activity should be minimized.

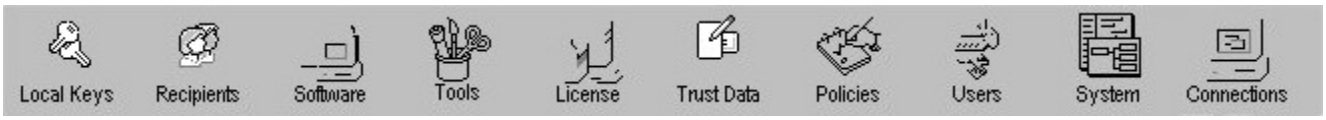
If you use a stand-alone PC with its own modem for Internet dial-up connection then the top option (Dial Up Modem) will be the best to select. You will have this choice during install, but you may change this setting at any time if your connection method changes.

In most other cases, the LAN Based Mail Server option will be appropriate. If you are unsure of your method of mail collection/delivery then the Mixed Dial-up and LAN/Dedicated Internet option will provide a suitable compromise, but ideally you should contact your Systems Administrator or InvisiMail Technical Support if you are unsure.
.

## Viewing mode

There are two view modes - standard and full.

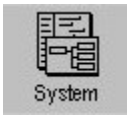

The standard view gives you access to the most used options.




The full view allows access via the toolbar to all Manager pages.

You can switch the modes by using the view mode check box on the Tools page. The check box allows you to start InvisiMail Manager in whichever mode is preferred. After any changes to this check box you should close InvisiMail Manager and re-open it to allow the new setting to take effect.

The Trust Data, Policies and Users buttons are used mainly in the Gateway and Network versions and their useage is explained in the appropriate Installer guides.




# System

The System button shows a page whose user functions are at the bottom - Service Status and Service Startup. By default, InvisiMail will load automatically when your PC boots up; you may turn this function off by using the radio button provided. You must then close InvisiMail Manager and restart your PC to effect the change.

The Service Status radio buttons allow you to stop InvisiMail protection instantly and also to restart the service of protection from within the Manager, without the need to shutdown or restart your PC. Use of this button obviously has significant implications for the email packages you have installed - stopping and/or starting the service will affect ALL your email programs not just a selected one. It is recommended that you close and then re-open your email programs after the selected change has been made.


# Connections

Connection proxy settings and Workstation IP port settings may be viewed and, if necessary, altered here.

The settings on this page are input automatically when InvisiMail is installed. They refer to your mail server settings and the means by which InvisiMail intercepts and secures your messages. In a stand-alone setup with a Dial-up connection and no other mail server-type software loaded these settings would not normally require any alteration.

For the installation of the Enterprise editions, the proxy settings will need to reflect the setup of your network mail arrangements:- whether you have inbound mail from one address only or you wish to allow multiple connections etc. Most of this setup can be performed during your install which is why we recommend you are fully cogniscent of your requirements and network layout prior to commencing - please read the install guide provided with the Enterprise Editions as it will save time later on.

It is inadvisable to alter any of these settings unless you are familiar with their concepts and useage or you have been advised on how to do so by your Systems Administrator or InvisiMail Technical Support.


# Trust Data

Trust Data is used by InvisiMail as part of the authentication process to indicate when an unauthorised person is attempting to impersonate a known correspondent.

When InvisiMail sends a message to an unknown user, InvisiMail generates a random token which is exchanged and automatically returned in all future correspondence. On receipt of a message InvisiMail will reference the trust token against its own record to ensure that there have been no changes. If a variation is found InvisiMail will know that it is not communicating with the intended recipient and will notify the user in the digital message signature attachment. This feature is only enabled in paid versions of InvisiMail.

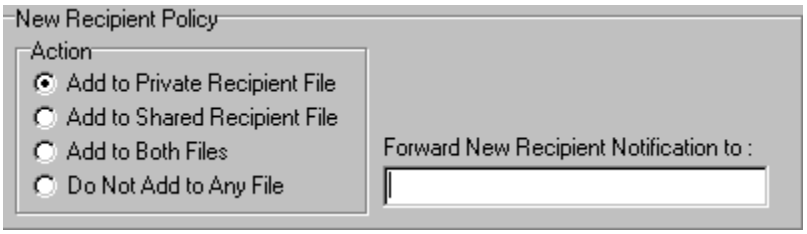
For added flexibility it is possible to manually verify the trust data with the intended recipient by looking in the Trust Data Menu of the InvisiMail Manager. You will find the trust data held for the recipients key reference and confirm this manually by calling and confirming that this is correct, much the same ways as a bank may confirm customer details prior to opening an account.


# License

InvisiMail automatically completes the licensing details section on upgrade from Intro to Deluxe, This section is only for use in the Network and Gateway editions of InvisiMail for adding additional licenses.

## Security Policies

A new policy may be created by clicking the Add Policy button on the lower left of the Policies screen and typing a new name for it.




The sub-section of the Policies dialog box shown above allows Recipient policies to be altered from the default which adds all new Recipients to the Private Recipient File.

An e-mail address may be supplied for notification of any additions to the Recipient lists; this would be of more use to System Administrators who wish to keep track of new Recipients than individual users who are likely to be aware of all their intended Recipients.

Encryption rules allow you in essence to turn encryption on or off as required.

Key Management allows for the use of different keys for different Policies. You may control the sending of your key by choosing to do so only in encrypted messages or only in plain text mesages; the default setting is to always send.

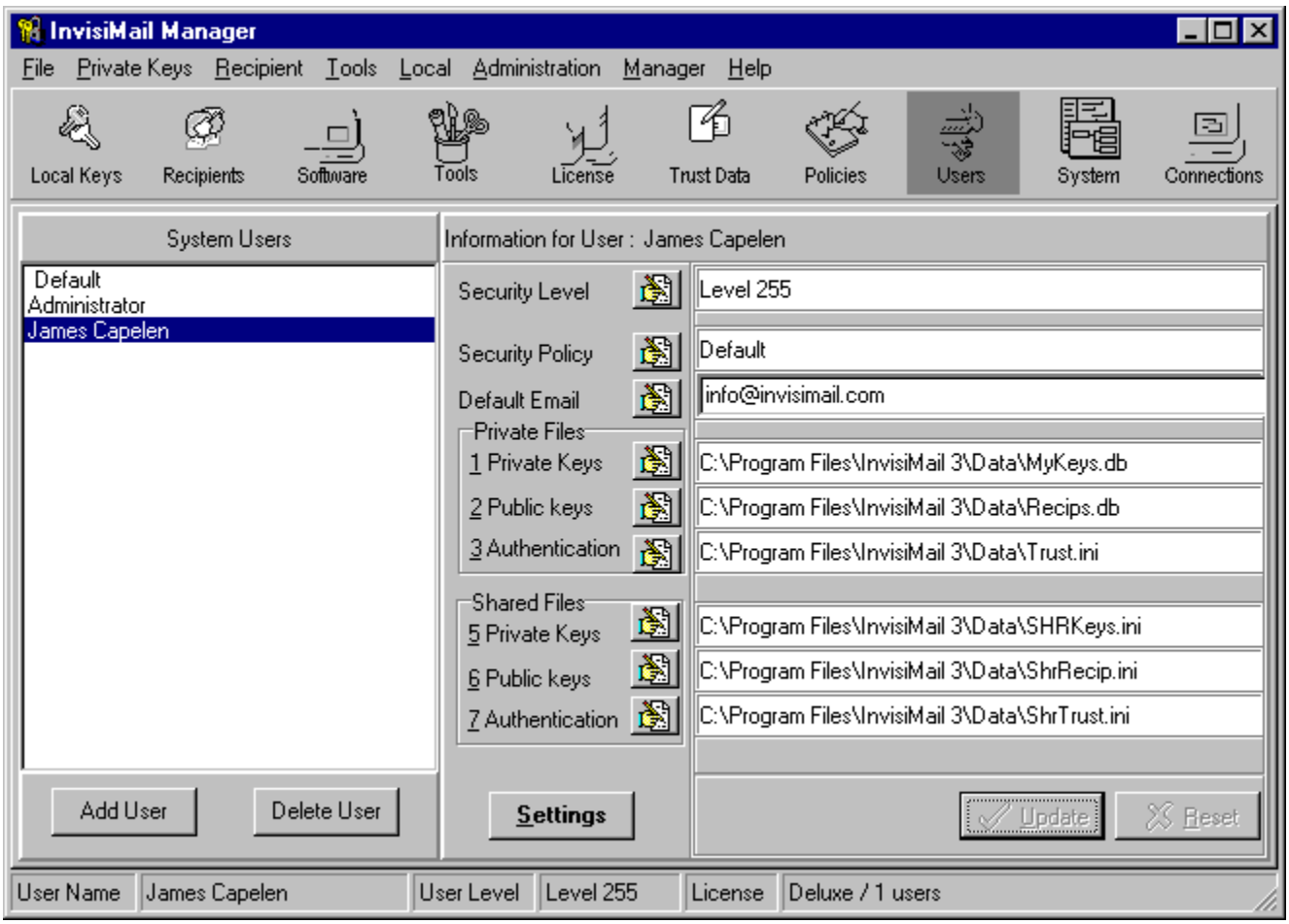
Receipts can be requested or provided as necessary.

The Outgoing message policy can be set to only allow emails to be sent if they can be encrypted for their destination or to allow passage of all emails.

Further options are available to Enterprise Edition users/administrators who can receive notification of authentication failures and rejected emails that have not been allowed by the Policy settings.

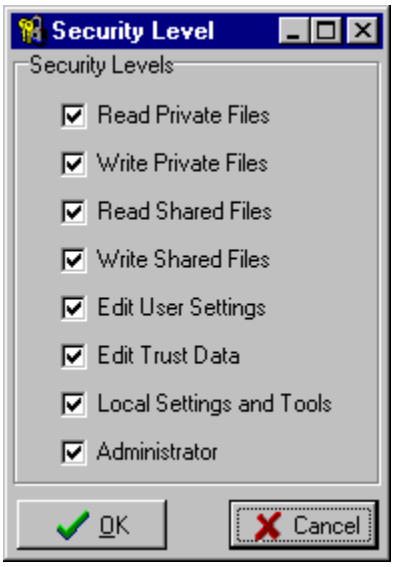
# User Options

There are a number of options available on this page for configuring security for individual users and the following is a step-by-step guide.



## Security Level

When InvisiMail is being installed, you are asked to supply a password to protect the InvisiMail files on your PC. You are given full access rights to the InvisiMail Manager and to those files by default. If there is more than one user able to access the Manager then their ability to see and make changes to Invisimail files and settings can be restricted. This is acheived by using the Security Level options screen on the Users page within InvisiMail Manager.




The check boxes shown above can be ticked or un-ticked as required and the security settings applied to individual users. As with all other types of access restriction, rights should only be granted to a user if that user really needs them; security breaches are far more likely to occur if users are given unecessary rights.

## Security Policies

Policies may be defined for use with groups or with individuals. They are assigned on the Private Keys page.

Most of the options available for Policies are for use with the Network and Gateway server editions only.

The drop-down menu is used to select the required policy (if you have not defined any then only the default policy will be available).

## Default E-mail address

The default address is set during installation, but may be changed at anytime using this button and text window. The Update button must be used after a new address is entered, else the original address will be retained.

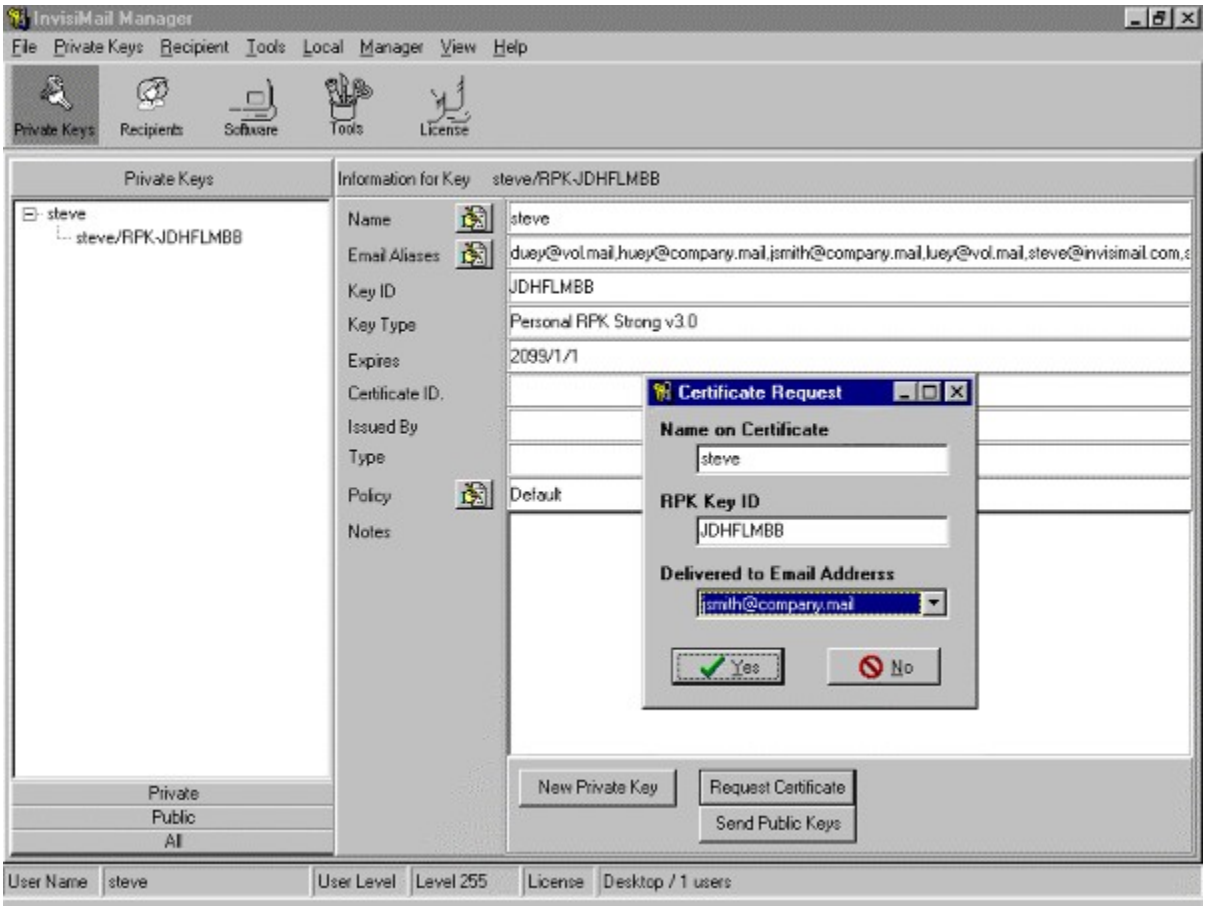
## Content Security

Just as InvisiMail seamlessly integrates with your email client, full support is provided for integration with Symantec's ACT! 4. This allows secure (607bit / 1279 bit) database synchronisation globally providing excellent additional functionality to this market leading product.

# Certificates

To assist in the confirmation of a user's identity, InvisiMail provides Certificates from the InvisiMail Certificate server.  A certificate is automatically requested on generation of public/private key pairs during the installation. It is also possible to request a certificate a later date should new keys be generated by simply clicking on the "Request a Certificate" button in the Private Keys menu, where upon the user is prompted to confirm which key the certificate will be associated with. InvisiMail will also identify any aliases that are associated with this key and ask for confirmation as to which e-mail address the certificate should be sent as shown below

**Requesting a Certificate**




On receipt of your certificate this will be included with your public key information in the header of every message sent so that users can confirm by looking at your key reference in their recipients list which will confirm the certificate.

## *Acknowledgements*

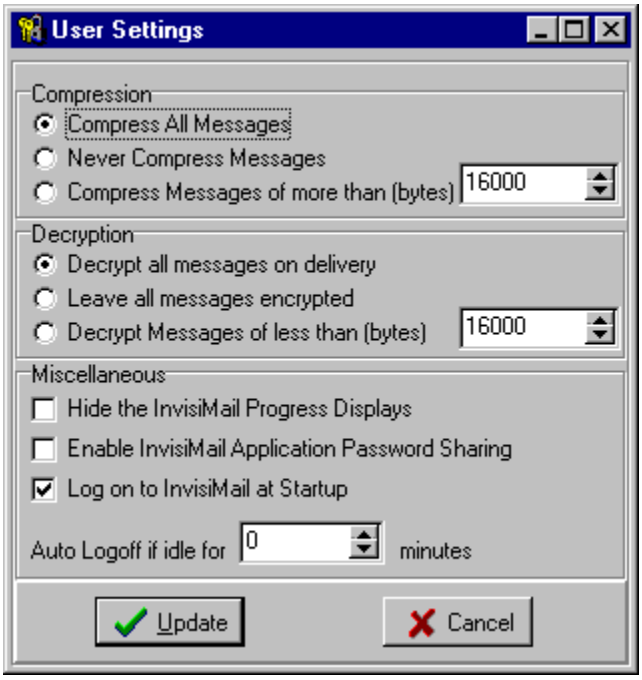
This product has been developed by Virtually Online Ltd



Cryptographic library (libeay32.dll) developed by Eric Young


RPK Encryption technology developed by RPK New Zealand
Copyright property of RPK International Ltd

# User Settings




You can choose options for compression (provided you have purchased a copy of InvisiMail), whether to decrypt your messages immediately or leave them safe until you are ready to read them. You may turn off Progress screens to make InvisiMail completely unobtrusive.

Auto logon and timed auto logoff functions are available in this release (v3.1). If Auto logoff is set to 0 minutes then InvisiMail stays logged on. The Enable InvisiMail Application Password Sharing function allows you to log on once at startup and thereafter any time you access the Manager program it uses your startup logon to activate the Manager without you retyping the password.

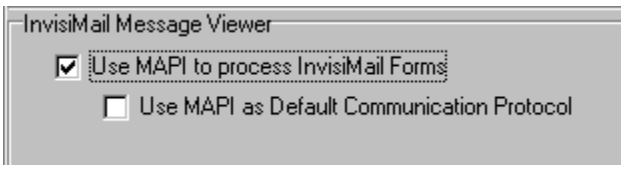
You must click on the Update button to activate any setting changes made here.

## Digital Signatures

InvisiMail now uses Industry standard DSA Key Signing. This protects your Public Key from tampering and man-in-the-middle attacks where a third party pretends to be a legitimate sender i.e. they are prevented from pretending to be someone else as their digital signatures wiil fail verification.

## MAPI / Outlook Forms

Under the title InvisiMail Message Viewer MAPI support can be enabled either just for viewing forms or for use as the standard message protocol.




This provides much wider support for e-mail clients - AOL, Exchange Client, Compuserve and any MAPI or Outlook compliant e-mail system.

IMAP4 Support has also been improved - works with Netscape and Outlook IMAP clients; includes an improved user interface.

## Updating from v2.1x, 3.0 to v3.1

It is always good practice to back-up your software prior to any software changes and we recommend as a precaution you should copy your InvisiMail folder before running the InvisiMail 3.1 installer file.

If you are upgrading from v2.1x then the v3.1 installer will prompt you to uninstall your old version, install v3.1 and then import your previous data.

From v3.0 , Version 3.1 will pick up your settings and seamlessly transfer your keys and recipients from the previous install. You should then send yourself a test message to check functionality.
(see Testing the Installation)

# What's NEW in **InvisiMail 3.1**

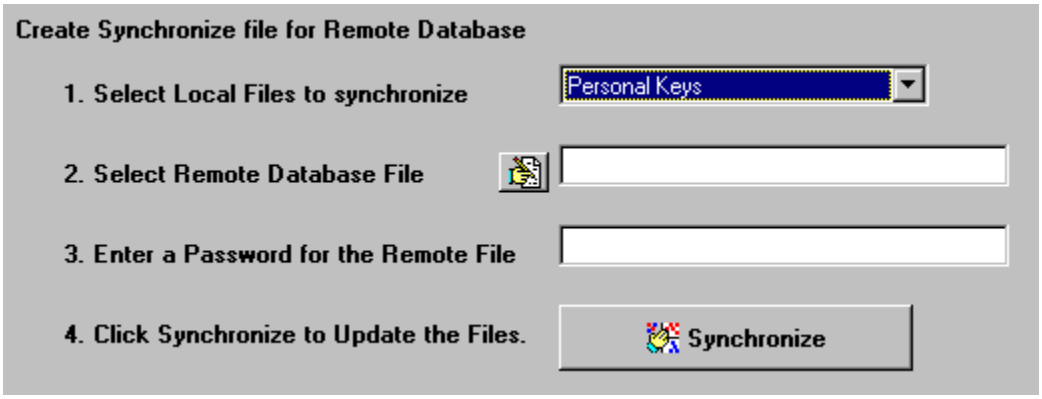
Performance has been increased by up to 400%; support for any MAPI or Outlook compliant E-mail system; Digital Key signing; supports integration with ActiveX clients development environments; improved IMAP support for Netscape and Outlook; Synchronization available between desktop and portables; improved control and sending options and -

## Encryption Desktop Utilities

Allows encryption of files and folders using Public keys and / or passwords. Maintain data structure when archiving and decrypting. Prevent theft of sensitive data from deleted files by secure file and folder shredding. Create and read .zip, .arj, .arc, and .cab files without the need for any other utilities. Works as a standard drag-and-drop style interface; intergrates with existing InvisiMail software.

# Synchronization

From the Manager menu a new option is available which enables mobile users and users who move between multiple sites to take advantage of the InvisiMail 3.1 Multiple Key Database.




The screen shown above will allow you to export the data files from one PC and then import them into the database on a second PC thus combining both databases. The combined data can then be exported back to the original PC giving both a synchronised database of keys and or recipients.

Lets go through this process step-by-step:-

On your local machine, pick the data you wish to export;Personal Recipients, Personal Keys, Shared Recipients or Shared Keys - in this case we will choose Private keys.

Choose where you wish to export to e.g to a file on a floppy disk.

Choose a password to secure the file and press Synchronize - this will export the secured Private Key data to file on the floppy disk.

Take the floppy disk to your remote machine;you may then synchronize the data from the first machine with the data from the second by specifying the second machine's Private keys in the Local Files to Synchronize box, choosing the path to the floppy disk file for the Remote Database File and entering your password. Pressing Synchronize will now combine the two files on the hard disk of the second machine and on the floppy disk as well.

If you wish, you may now return to the first machine, repeat the procedure using the newly synchronised file as the Remote Database File and press Synchronize; both PCs will now have identical Private Key references.

You should always restart your PC after making changes to the InvisiMail setup to ensure all changes are recognised.