

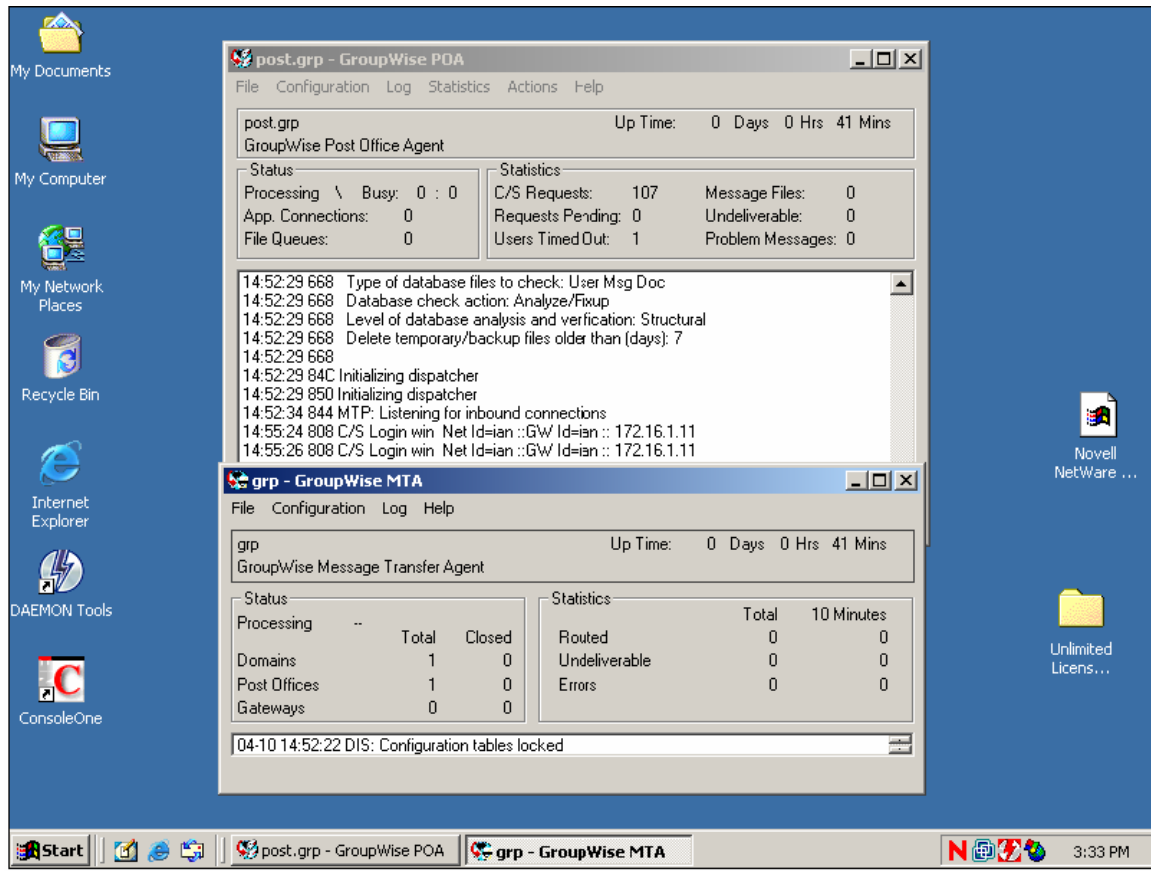
Introduction

GroupWise, is currently the Novell E-mail solution, and is a favorite of Novell Administrators largely due to its reliance on the Novell directory. However the protocol and mail interface is not very original, the main interface is based on the Microsoft Mail engine, and is backed by a simple Database shared on the edirectory server. This allows us a great deal of flexibility in dealing with GroupWise from a forensics point of view, due largely to the requirements on the Microsoft mail platform a lot of the general forensics rules applied to Outlook and Outlook Express can be applied to GroupWise.

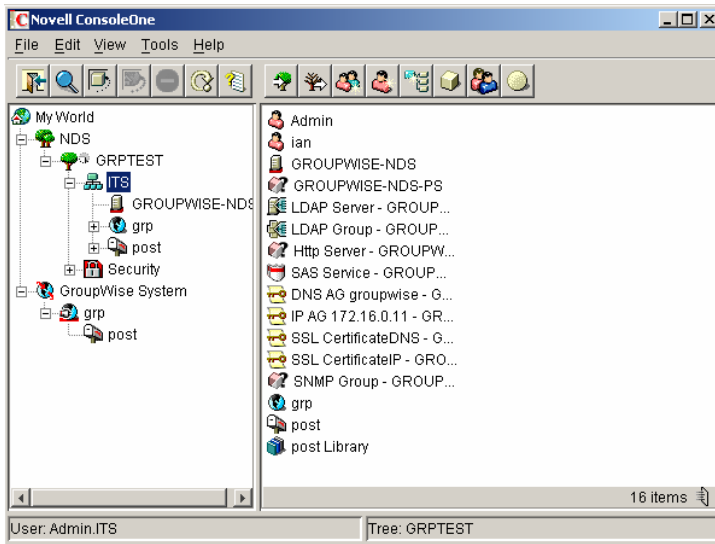
Basics of GroupWise

GroupWise objects are added into the edirectory, the first is the Domain Directory, this object and its accompanying database controls all information on what users and there properties are accessible to the system, the second is the Post office. The post office is the main terminal for e-mail sending and delivery, in a fully qualified e-mail system with internet mail all outgoing and incoming email handled by the post office is sent to a internet gateway, however GroupWise can function as a internal e-mail system without the need for the external support

There are two programs that are required for GroupWise to access the POA (Post Office Agent) and MTA (Mail Transfer Agent) all the GroupWise objects are components of E-directory so therefore it is not critical that the agent software be consistent, for that reason Novell currently has loadable agents for Netware, Windows and Linux however it is required that E-directory be installed on the Linux or windows server to be able to host the GroupWise directory.



Windows Server Running GroupWise POA's and MTA's

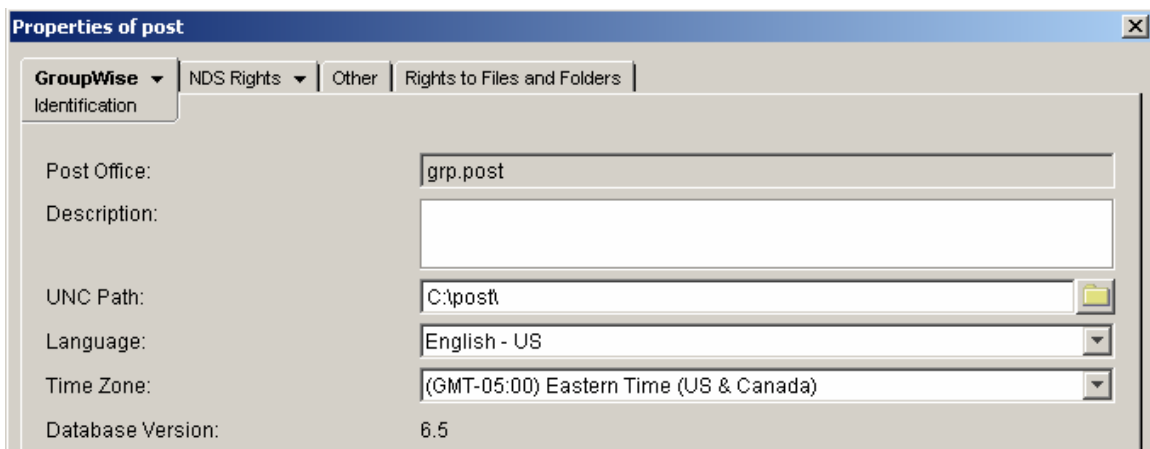


Console1 Illustrating the GroupWise Objects

Forensics Procedure

For the purposes of never working on a original copy of the software the examiner should copy the following files out of the directory's as they make up the bulk of the GroupWise information, however most of the forensics information is based on the system as a whole. So therefore making a backup of the Post Office and Domain directories and then replacing the files if necessary will allow for a the forensics procedure to be followed

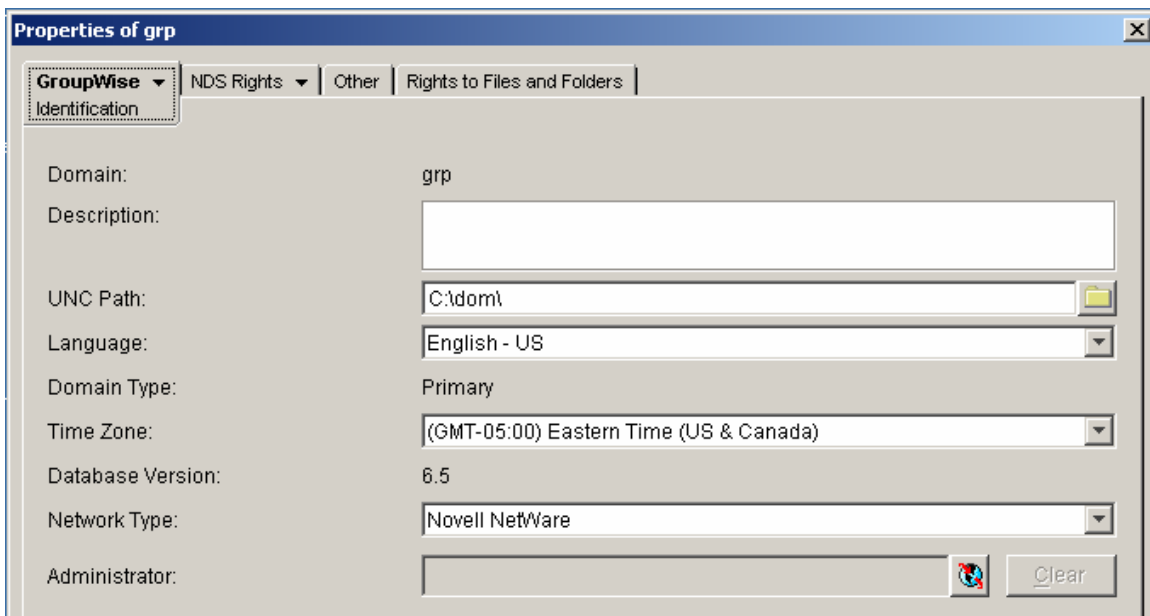
The location of the files should be noted by the administrator at the time of install. However if its not, the information can be viewed via console1 by clicking on the domain object or the post office object.



The screenshot shows the 'Properties of post' dialog box. The 'GroupWise' tab is selected, and the 'Identification' sub-tab is active. The fields are as follows:

Post Office:	grp.post
Description:	
UNC Path:	C:\post
Language:	English - US
Time Zone:	(GMT-05:00) Eastern Time (US & Canada)
Database Version:	6.5

Post office Properties



The screenshot shows the 'Properties of grp' dialog box. The 'GroupWise' tab is selected, and the 'Identification' sub-tab is active. The fields are as follows:

Domain:	grp
Description:	
UNC Path:	C:\dom
Language:	English - US
Domain Type:	Primary
Time Zone:	(GMT-05:00) Eastern Time (US & Canada)
Database Version:	6.5
Network Type:	Novell NetWare
Administrator:	

Domain Properties

Nexic – The FTK of GroupWise.

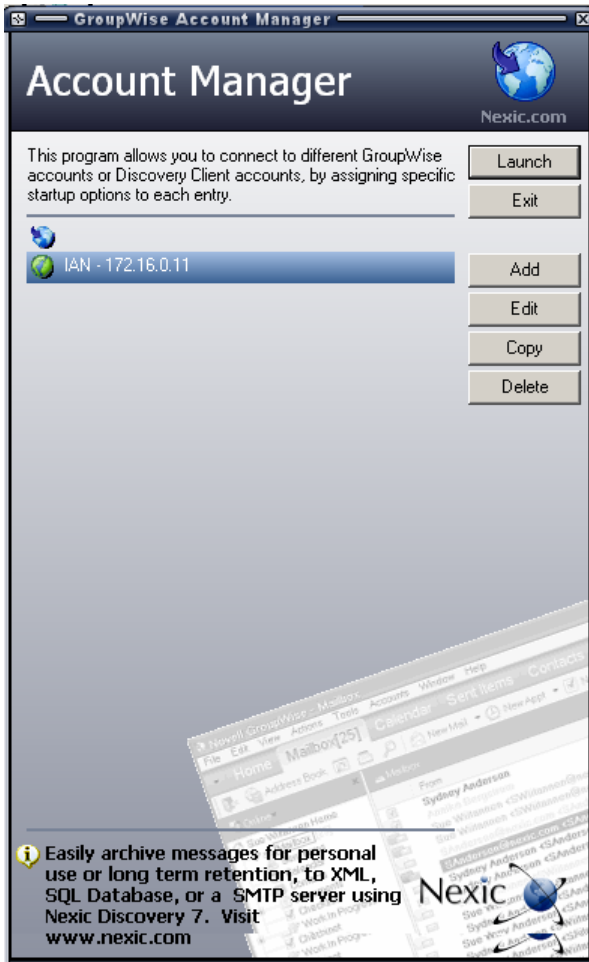
The main problem with forensics on multi-user e-mail systems (especially with Lotus Notes and GroupWise) is the interpretation of the database file, or more specifically what “suspicious” messages are going to what user, and providing to court standards that the e-mails in question did indeed belong to the user being investigated.

To solve this problem forensics companies like Nexic (makers of the GroupWise forensics software) have designed a program that will allow an administrator to enter a user’s GroupWise e-mail view, without changing the password. Effectively allowing the investigator to see as the user sees their e-mail inbox well still allowing the investigation to proceed without the suspect’s knowledge.

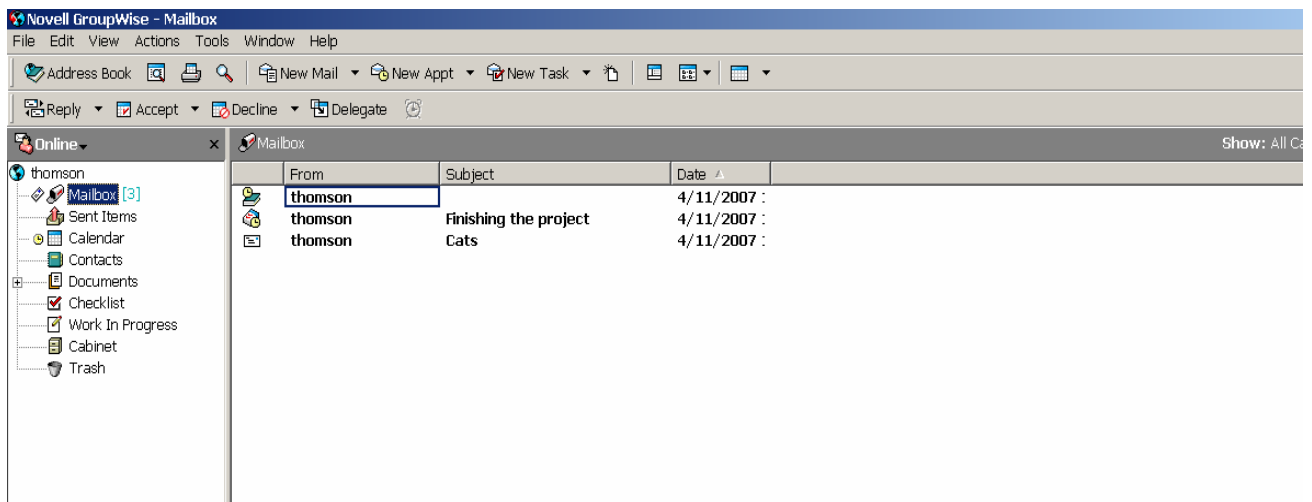
This has great advantages over Microsoft’s message tracking tool due to the fact that the investigator can get a greater sense of how the suspect thinks and stores e-mail.

Also Nexic will allow the investigator to export e-mails to a sterilized source for further investigation.

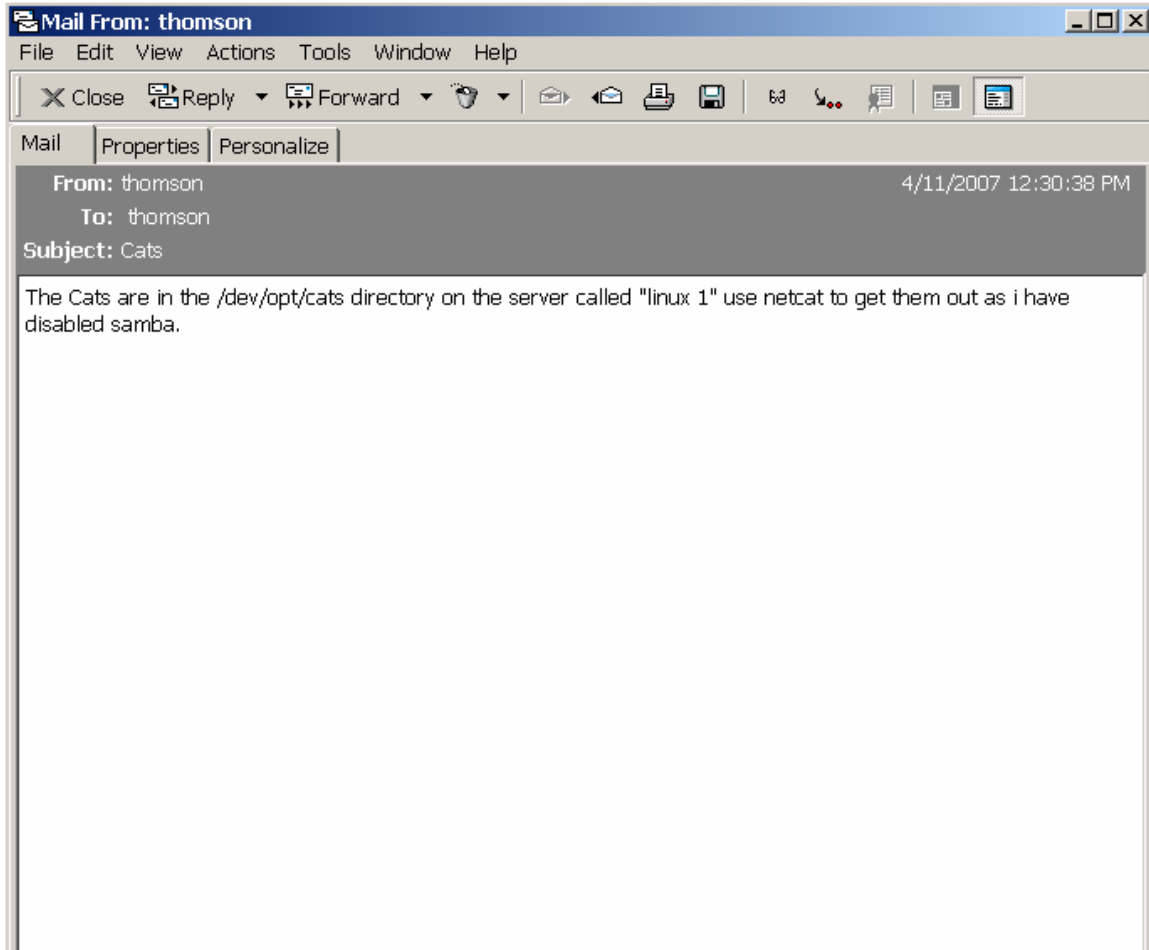
Nexic works by generating a secure Key, and asking a user with admin privileges what mailboxes should the investigator (through the investigative control program) should be allowed to investigate, although the investigator can add more mailboxes through the discovery program this can only be accomplished if the account the investigator is using has admin privileges



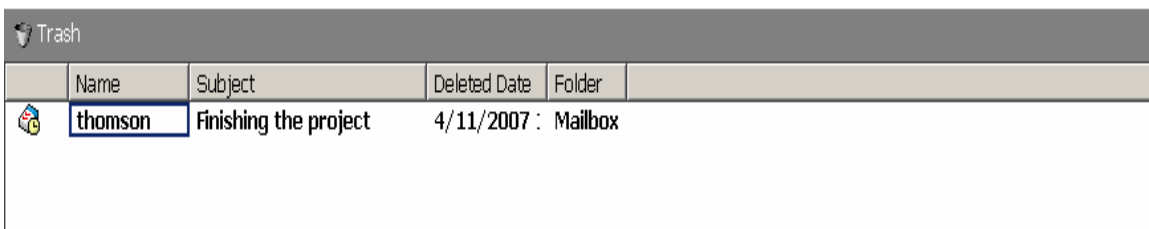
Nexic after being configured with the GroupWise server details allows the administrator a list of users on startup. By simply double clicking on the icon of the user account the investigator can view the mailbox of the suspect



Once in the user's mailbox the investigator can view the messages and conduct the investigation as if they were investigating themselves.



Although Nexic does not offer a feature to undo any changes an investigator makes to the users mailbox groupwise has a built in trash feature that will allow us to recover deleted messages



Message Headers and Properties

As with all e-mail systems GroupWise does attach message headers to documents however like most network e-mail systems it does a effective job of hiding the headers from the user, even if the message is exported or saved, a version of the message headers can be viewed by clicking the properties tab on any GroupWise message.

Mail	Properties	Personalize
Mail Envelope Properties (461D0D2E.3E7 : 12 : 43293)		
Subject:	Cats	
Creation Date	4/11/2007 12:30:38 PM	
From:	thomson	
Created By:	ian.post.grp	
Recipients	Action	Date & Time
post.grp	Delivered	4/11/2007 12:30:38 PM
Admin ()		
ian (thomson)	Opened	4/11/2007 12:34:46 PM
Post Office	Delivered	Route
post.grp	4/11/2007 12:30:38 PM	
Files	Size	Date & Time
MESSAGE	435	4/11/2007 12:30:38 PM
Options		
Auto Delete:	No	
Expiration Date:	None	
Notify Recipients:	Yes	
Priority:	Standard	
ReplyRequested:	No	
Return Notification:	None	
Concealed Subject:	No	
Security:	Standard	
To Be Delivered:	Immediate	
Status Tracking:	Delivered & Opened	

The properties values are stored by the server and without manipulating the database cannot be altered.

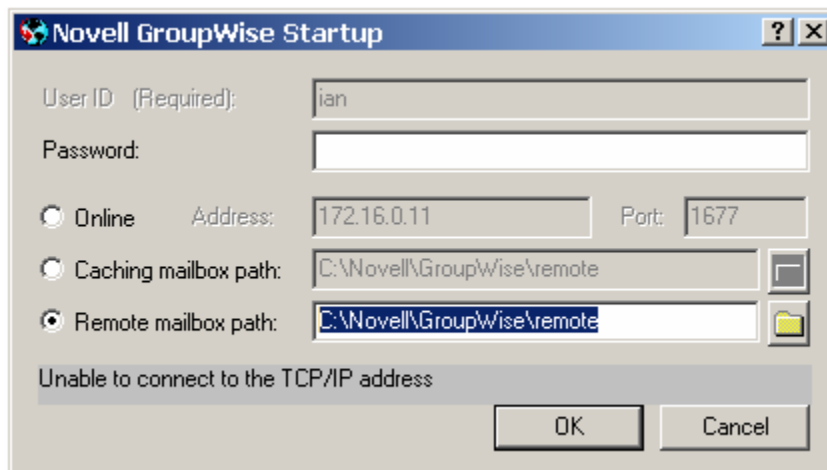
Storage of Profiles

Differing slightly from its windows counterparts the GroupWise storage system does not store profile information or mail box information on the user's home directory and then differentially change the information onto the server. All the information is stored on the server and then records (mail items, calendar events ect) are retrieved as needed. This was a major downfall in GroupWise 5 due to the fact that it was designed at a time when 10mbps was the standard duplex for networking. However since the introduction of GroupWise 6 and 7 the standard has remained the same, which allows forensics professionals a better means of investigating users GroupWise directories.

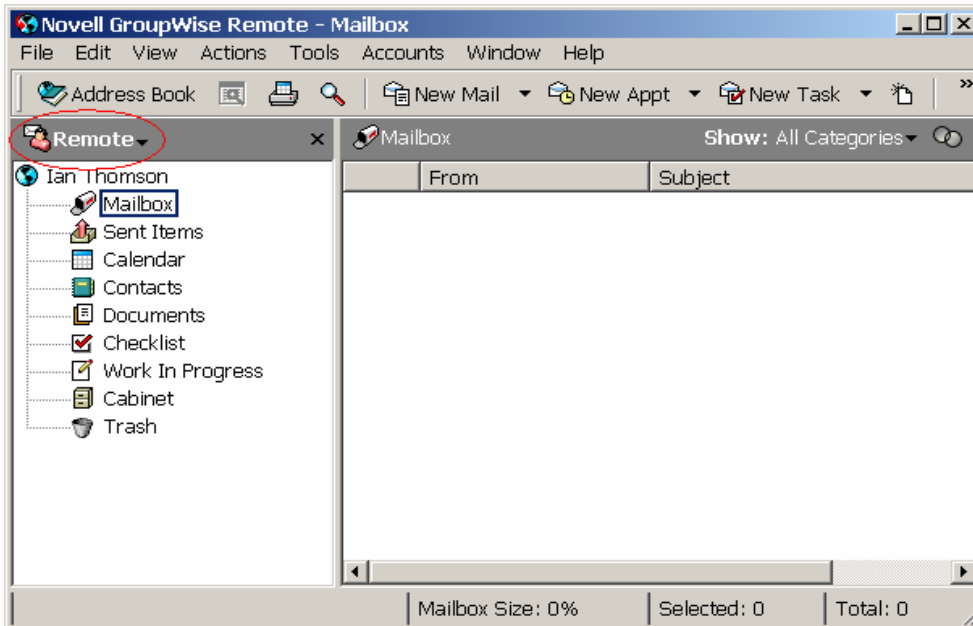
Offline GroupWise Profiles / GroupWise without a server

It is entirely possible to use GroupWise simply as a client without the server and edirectory backbone, however it is required that the user specify a GroupWise path. This path is stored at whatever directory the creating user decides, however by default it is set to C:\Novell\GroupWise\remote

One way to tell if the user is using a remote GroupWise profile is if the following window is displayed when GroupWise is launched



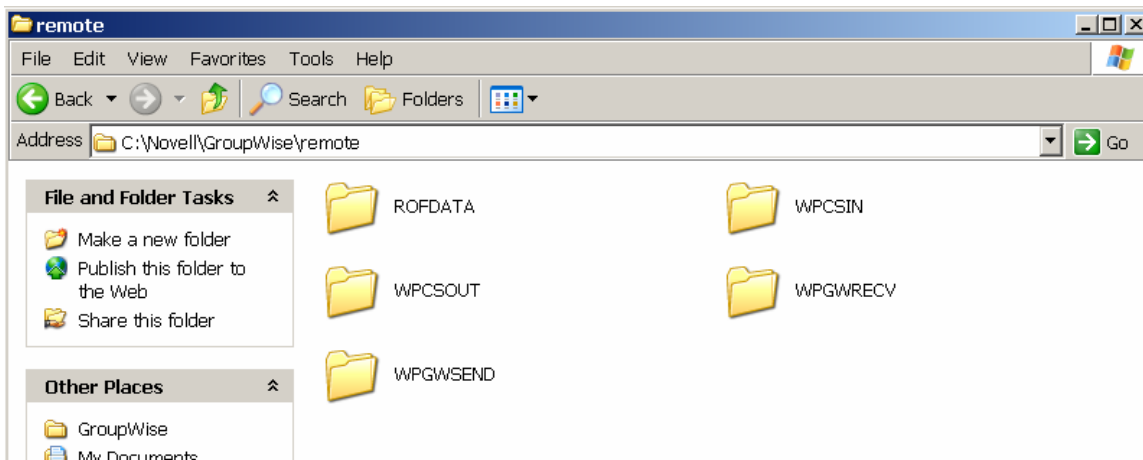
This will also point you to where the profile exists as by default it will display the last logged on profile



GroupWise remote mailbox note the user icon indicates remote connection

Contents of a GroupWise mailbox

The groupwise mailbox generally contains 5 Main Folders these folders contain all the information on the mail exchanged



WPCSIN – Contains the Inbox Database

WPCSOUT – Contains the Outbox Database

WPGWRECV – Contains information Received

WPGWSEND – Contains information sent

All of these folders when properly populated will contain a collection of database files, if necessary these files can be opened with a database editor.