

Introduction

As with all network services, it is important to maintain a confidential and secure operating environment, with GroupWise's heavy inclusion in the edirectory security is insured. Just as exchanges security is generally as secure as the Windows domain version that it is hosted upon. For this reason there is little configuration required to make GroupWise secure, it is more important however to insure that the main edirectory remain secure.

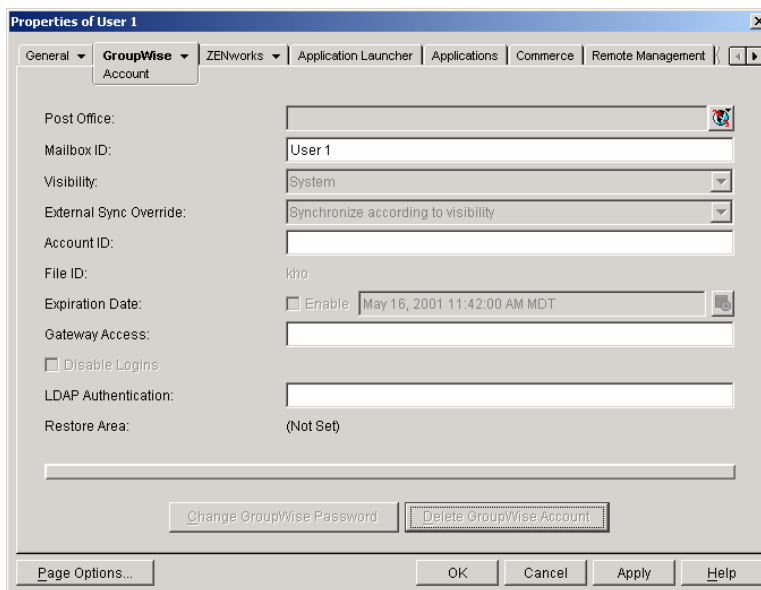
Major Problems and Threats to Security

The major problems that threaten the security of the GroupWise system are the following

- Password Security
- SPAM
- Denial of Service

Password Security

Password in the GroupWise system is coupled with the password in the edirectory and in properly designed networks single sign on is implemented; this allows users to maintain one password for all there Novell services. However some users prefer to confirm there password when accessing GroupWise, to do this simply change the GroupWise password by accessing the GroupWise tab on a console 1 user's object. Making the password different then the edirectory password will ask the user to re enter there password when the GroupWise program is accessed.



Change GroupWise Password Dialog

SPAM

As with the Microsoft exchange and lotus notes platforms spam e-mail is a large problem, however there are several solutions that integrate very well with the edirectory however they are not well publicized



GWGuardian is by far the most intuitive program and is one of the only products supported and featured by Novell. This product has an intuitive web interface that allows users to view there quarantined messages by logging into a secure environment that prevents viruses. It also allows personalized rules and a corporate wide spam rules system.

The screenshot shows the GWGuardian web interface. At the top, there is a navigation bar with buttons for 'Open', 'Refresh', 'Refresh', 'Delete', 'Update', and 'Purge deleted'. Below this is a table of quarantined messages. The table has columns for 'Category', 'To', 'Subject', 'Date', and 'Size'. The messages are listed as follows:

Category	To	Subject	Date	Size
Goods	mckenna@g...	mckenna, Lose Weight Without Dieting	1/3/2001 11:09:4...	3 KB
Money	lubo@gm.ga...	fountain of youth/a new body!	7/10/2003 1:20:3...	3 KB
Health	fred@gamem...	Food: Online Prescriptions. They're READY! njoyd...	7/10/2003 3:17:3...	6 KB
Health	roya@gamem...	Half Off All Prescription Medic! [qd rllant	7/10/2003 3:21:5...	10 KB
Goods	jeeds@gamem...	\$80 Offer to print postage with Stamps.com	7/10/2003 4:21:2...	0 KB
Goods	mary@gamem...	\$80 Offer to print postage with Stamps.com	7/10/2003 4:21:5...	0 KB
Goods	ncendog@g...	No instructions needed	7/10/2003 4:27:5...	3 KB
Goods	eagle@gamem...	Working hard lately?	7/10/2003 4:28:2...	3 KB
Goods	hardired@g...	Food: You may want to reboot your computer	7/10/2003 4:23:4...	2 KB
Goods	denjeann@g...		7/10/2003 4:29:2...	3 KB
Goods	langford@gm...	NEW: Animal's eyes (must be 18 years old)	7/10/2003 8:22:1...	7 KB
Money	zeus@gamem...	Refinancing? Get a F R E E Quote on any Mortgage..	7/10/2003 10:45:1...	3 KB
Money	clif@gamem...	weight loss while you sleep, a leaner & healthy b...	7/11/2003 2:20:4...	3 KB
Money	182245941@...	ALERT: Mortgage Rates On The Rise ... Act Now! %...	7/11/2003 4:23:1...	9 KB
Goods	allenj@gamem...	We Make the Leaders Compete for YOUR Business...	7/11/2003 8:15:0...	2 KB

At the bottom of the table, there is a small button that says 'We Make the Leaders Compete for YOUR Business? annou...'. Below the table, it says 'Quarantine: 21 Message(s)'.

GW Guardian Spam Box

GWGuardian is an expensive system, and if the GroupWise user base is examined it is discovered that GroupWise is used by educational institutes and require an easy administration e-mail system. Therefore GWGuardian is used primarily by large educational institutes with large IT Budgets.

Denial of Service

With most educational e-mail systems a large amount of attacks are internal denial of service attacks, therefore it is very important to outline the main problems associated with GroupWise systems. The first being its heavy reliance on Microsoft mail standards, this allows the GroupWise system to share several of its windows counterparts vulnerabilities.

Therefore it is advisable that the GroupWise system be configured to use a non standard port and then use port forwarding, to allow access.

As well to prevent denial of service usernames with direct access to the GroupWise shares discussed in the forensics article should be limited, preferably only to the admin account, helpdesk users will still be able to perform administrative tasks, allowing for decreased point of access and therefore decreased denial of service.