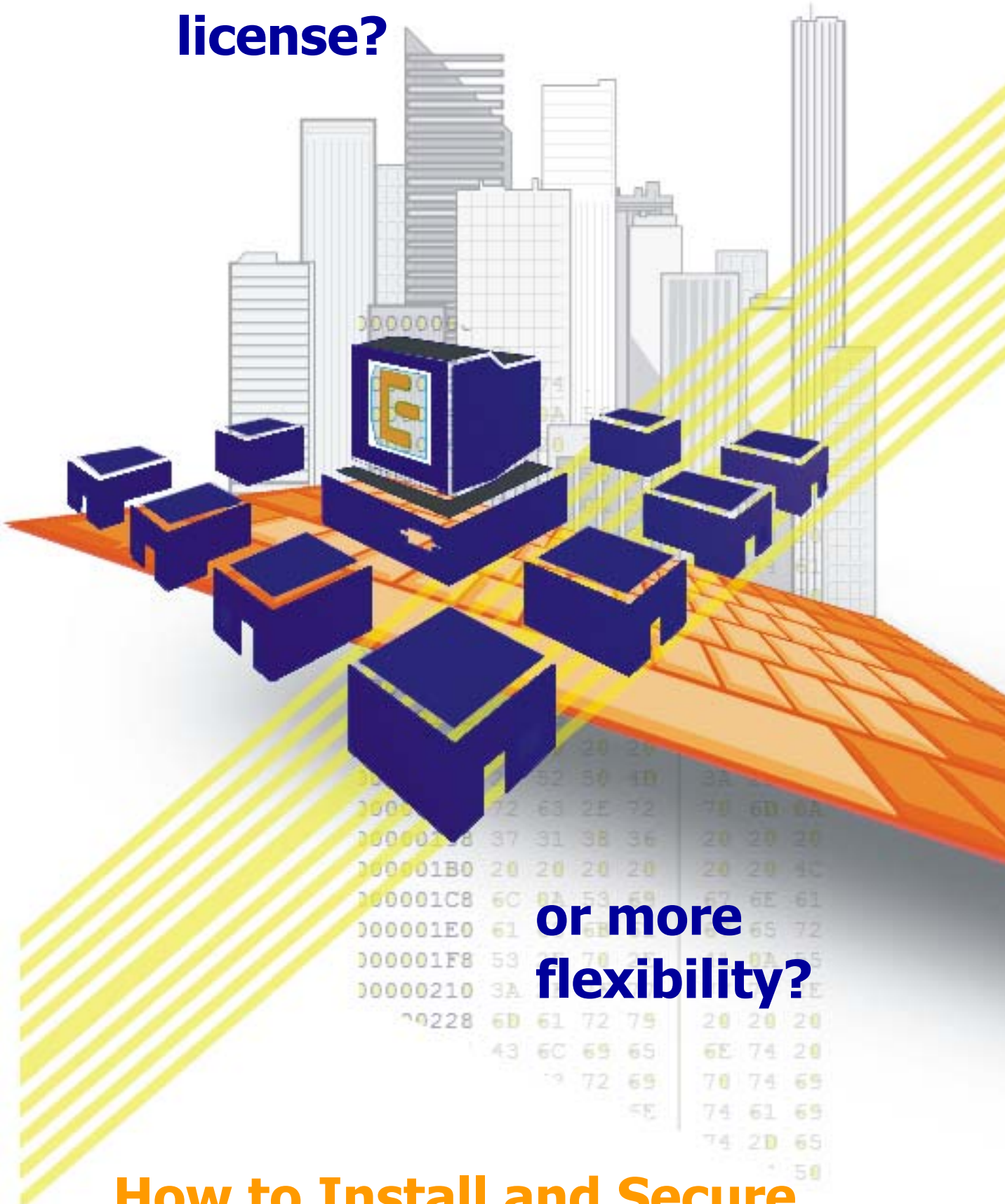
Need a license?



or more flexibility?

How to Install and Secure eGroupWare

eGroupWare, why e?

decide for yourself, we could never pick one!

enterprise, extended, extreme ...

groupware

For information on obtaining permissions for use of this material from this work, please submit your request to

Reiner Jung
rjung@expl0it.de

 **expl0it labs** offer packaging and open source security development

 **expl0it press** is responsible for publishing HOWTOs, white papers and more

 **expl0it consulting** offer security consulting in the enterprise

Date published 5-Jan-05

Table of Contents

1 Introduction

eGroupWare is a groupware package programmed in PHP. It is open source software that can be installed on most operating systems, such as Windows, Mac, Unix, BSD and Linux. It is designed to run alongside your existing software (such as your database and mail server). The target of eGroupWare is to fulfill the requirements of enterprise environments in a groupware package while retaining the security and modularity of open source software. eGroupWare includes all of the applications that are needed to setup a complete office workplace. The long-term vision of the eGroupWare workplace is that 80 percent of an employee's business needs can be satisfied from within the groupware suite.

1.1 What will this book cover?

This book will cover the setup and security steps that should be followed when you install eGroupWare in your organization. The setup of eGroupWare itself is only a small part of what must be done to have a secure and available groupware solution – you must also perform such tasks as deciding what your update strategy will be, planning your firewall setup, and configuring your system to be resistant to intruders. This book also gives a short overview of some of the differences you may encounter when installing eGroupWare on varied operating system platforms; however, due to the myriad operating system and software configurations that are possible, it is by no means comprehensive. Please consult your system's documentation or post a question to the appropriate eGroupWare developer mailing list if you need help.

1.2 Who should read it?

Experienced and inexperienced eGroupWare users alike should read this book. The user must have a certain degree of comfort using his or her operating system, as this book will not cover operating system basics in any detail. However, it will give useful hints as to how you can better and more securely set up your operating system environment. Advanced users will find customizable example scripts (such as for iptables or aide) which can be modified as desired to suit their requirements.

1.3 Document convention

This manual uses different fonts, styles and icons to represent different things. Following are the style conventions used.

cursive

Cursive text represents command line operations.

`script`

Fixed-width font denotes the content of configuration or script files.

Wizard icons point you to download areas at http://www.example.com/files. At these places you will find some example configuration files that you can modify to suit your needs.

Information icons mean that the directory /var/www/html/egrouopware/phpgwapi contain additional documentation for the current topic (your path may be different).

Note icons are helpful reminders

Warning icons indicate important things you should be aware of

Caution icons denote very important things you absolutely must do!

Penguin icons denote actions you should take on a Linux or Unix operating system.

Windows icons denote actions you should take on a Windows operating system.

1.4 About the author

Reiner Jung has worked as a freelance IT consultant and security project manager for more than 14 years. He has experience with classical operating systems such as Netware, Windows, and Unix, but recently has preferred to work with OpenBSD and Linux. In 2004 he founded his own security consulting company, expl0it, based in Europe and South America.

2 Installation Checklist for eGroupWare

This list will give you a short overview of what you need to do to run eGroupWare. You don't need a compiler to install eGroupWare. eGroupWare is composed only of PHP, HTML and image files.

What you need to run eGroupWare	Example software	Check the requirements
You **need** an operating system like the following:	Linux, Unix, *BSD MAC WIN NT / 2000 / XP	☑ ☐ ☒ ☐
eGroupWare **requires** a web server. Here are some examples:	IIS Roxen Apache 1.3 or 2.0	☑ ☐ ☒ ☐
eGroupWare **requires** a database:	MYSQL MS-SQL PostgreSQL	☑ ☐ ☒ ☐
If you want to send mail with eGroupWare then you need an SMTP server such as:	Exim Postfix Sendmail	☑ ☐ ☒ ☐
If you want to use eGroupWare as a POP or IMAP mail client you need a corresponding server such as:	Cyrus Courier Dovecot UW-IMAP	☑ ☐ ☒ ☐
eGroupWare **requires** PHP:	PHP > 4.1 required. PHP > 4.2 recommended.	☑ ☐ ☒ ☐

3 Express Install HOWTO

This HOWTO will give a short introduction to the steps necessary for setting up eGroupWare. eGroupWare installations can be done in less than 10 minutes. However, unless installing eGroupWare as quickly as possible is absolutely necessary, it is recommended you go through this full book to ensure that your system is properly set up and secured.

1) Download the eGroupWare packages from the Sourceforge download area[1]. At the moment eGroupWare packages are provided at the project page zip, tar.gz, bz2 and rpm formats. Some Linux and Unix distributions, such as Mandrake, Debian, Gentoo, SUSE and FreeBSD provide customized packages designed to work with their distribution (for instance, they will correct the installation paths of the packages and ensure dependencies are met).

2)  Install the packages on your server in the webserver root (recommended) or any other directory you wish to use. The RPM package from Sourceforge will use /var/www/html as its installation path.

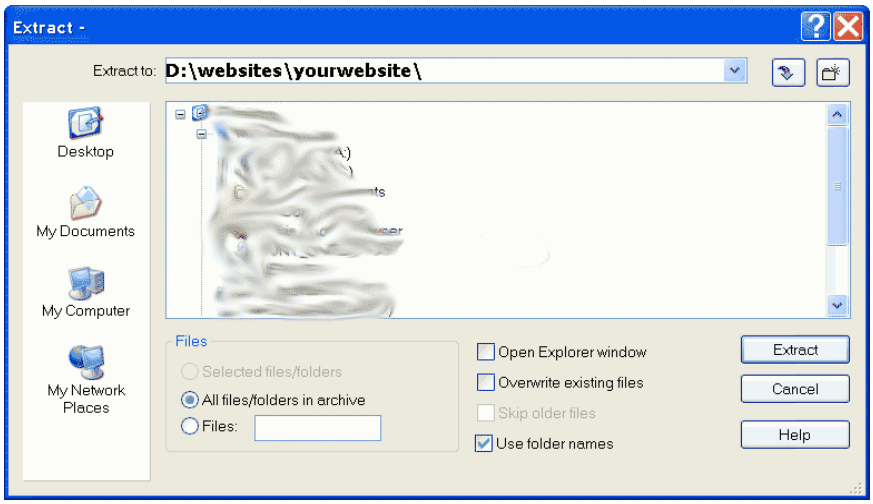
[root@server tmp]# rpm –ivh eGroupWare-x.x.xx.xxx-x.rpm

To install any other kind of package of eGroupWare, copy the package to the web server root directory, change to that directory, and extract the package.

[root@server tmp]# cd /var/www
[root@server www]#tar xzvf eGroupWare-x.x.xx.xxx-x.tar.gz

 Using a program like Winzip[2], unzip the file to any folder that is under your web server's root. In other words, the folder you choose must be accessible from the Internet. Make sure you keep the existing folder structure when you extract the zip file (the "keep folder names" option should be checked in WinZip in the Extract dialog) and your installation will look something like this: D:\websites\yourwebsite\eGroupWare\(all the files in the eGroupWare zip).

1 http://www.sf.net/projects/egroupware
2 http://www.winzip.com

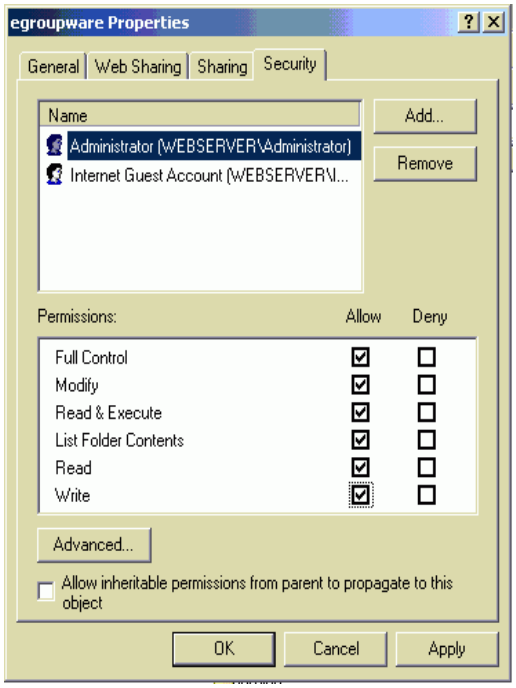


3) Change the permissions on the files in your eGroupWare installation. Use chown and chmod to do this (see the man pages of chown and chmod if you need help). Which user and group should own the files depends upon your particular operating system. Probably you will want to have root be the user owner and the web server's group be the group owner. Try using the recursion flags to both of these commands to make things easier.

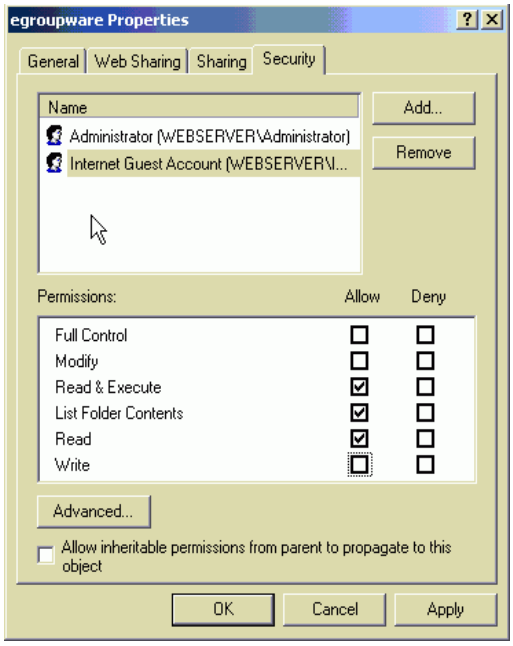
- Your admin user should have read and write permissions.
- The user under which your web server runs should have read access only. Your web server user only needs write permission on the fudforum folder.

Set the proper permissions for the eGroupware files.

The Administrative user needs to have at least **read** and **write** permissions.



The Web user (Internet Guest Account) needs to have read permission.



The Web user needs read and write permissions for the FUDFORUM only!

4) Ensure that your web server and database server are started.

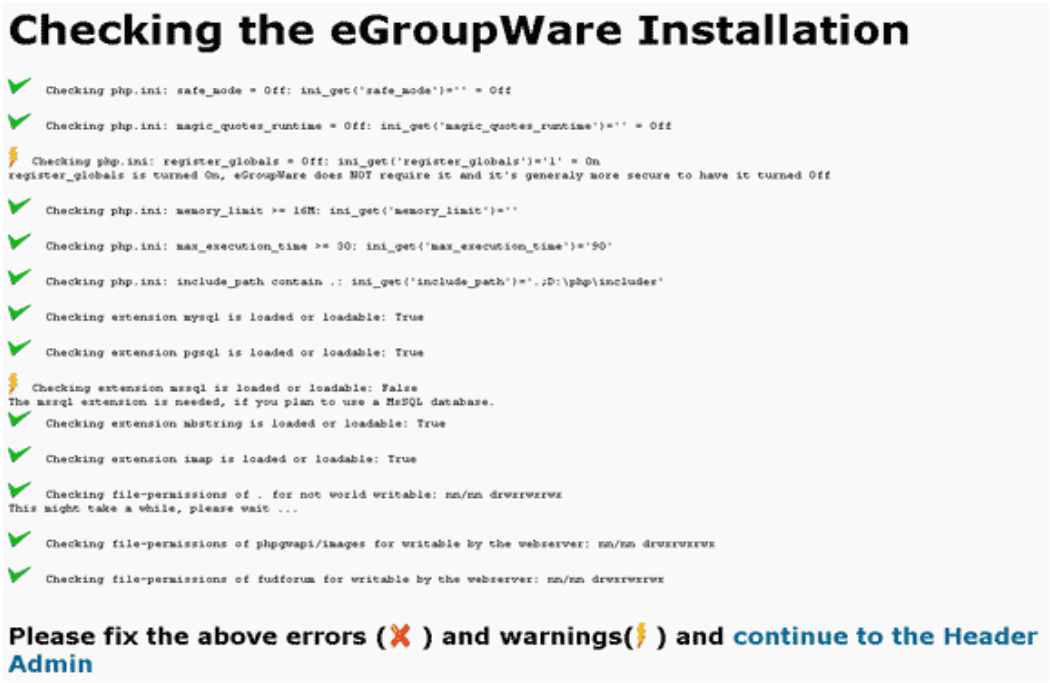
5) Point your browser to the URL http://<your_server_address>/egroupware/setup.

Depending on your web server setup you may be required to add "index.php" to your list of default documents. You may also be required to add a trailing slash to the URL above.

6) The check install script should start automatically.
- Wait until the script is finished, then correct any errors that are shown.
- After fixing any errors, reload the page to check your installation again.
- When there are no errors left, scroll down and click "Return to Setup."

You may have a couple of things that do not resolve completely. For instance, the **register_globals = on** setting in your PHP.ini file (Usually under C:\WINNT) may need to be changed. Some scripts require this to be on and some require it to be off. If you turn it off, other parts of your website that use PHP may not work. The sure way to find out is to set it the way eGroupWare recommends (off) and check your other sites. If they no longer work properly, set the value back to on. Please note: eGroupWare does not require this to be set to off!

Also the MsSQL (Microsoft) database extension will not be loaded if you are using MySQL!



When all conflicts are resolved you can click "continue to the Header Admin."

7) Start the Header Admin configuration.

- Fill out all of the fields.

Server Root – This is the "root" of your eGroupWare installation, i.e. D:\websites\yourwebsite\eGroupWare.

Include Root – make this the same, i.e. D:\websites\yourwebsite\eGroupWare

(Please note: **this is not your .com address or other FQDN**, it is the actual directory path to you eGroupWare installation.)


Don't forget the password. It will be encrypted and will not be recoverable later


Choose the option to "Download" the header.inc.php file and save it to the root directory of your eGoupWare installation (example /var/www/html/egroupware). Give the web server the right to read the file.


Choose the option to "Download" the header.inc.php file that you have just created, and either save it to the root directory of your eGroupWare installation (if you have access to the server), or upload it through FTP to that directory.

- Click continue

8) Login to Setup/Config Admin.

9) Create your Databases / Tables.
   - Fill out the form with your database root username and corresponding password to create your database automatically
   - Continue to create the database
   - Re-check the installation
   - Continue to create the tables

 This should be very simply if you know the name and password for your MySQL server. Fill in the information and "Create Database."

When you click "Re-check My Installation" you will probably see that you "have no applications installed" and be given the option to "install the core tables and the admin and preferences applications." Go ahead and install those tables.

***Note "TROUBLE SHOOTING" section – if you receive errors.**

10) Edit Current Configuration.
   - Create a directory outside your web server root and give the weserver user the rights to read, write and execute in this directory. As an example, when your web server root is /var/www/html, you could create the folder under /var/www/files

 This means to create a folder/directory that is not under your D:\websites\yourwebsite\eGroupWare directory tree. For example if your "root" installation is at D:\websites\yourwebsite\eGroupWare, you will want this directory/folder at something like D:\websites\yourwebsite\new_directory. Once the directory/folder is created make sure the Web user has permissions to read, write, and execute in this directory/folder.

11) Create your Admin User.
   - Do not use this account as your primary, day-to-day user account. It should be used as a backup user and for initial setup only

12) Manage Languages.
   - Install the languages which you want to use.

13) Manage Applications.
   - Uninstall applications which you don't want to use

14) Login to eGroupWare.
   Point your browser to http://yourservername/egroupware

4 Migrating Your Installation from phpGroupWare to eGroupWare

Download the necessary packages from our page and install them as described in Section 2. Copy the header.inc.php file from your phpGroupWare directory to your eGroupWare directory and edit the following lines in **header.inc.php** (your paths may vary slightly):

From:

```
define('PHPGW_SERVER_ROOT','/var/www/html/phpgroupware');
define('PHPGW_INCLUDE_ROOT','/var/www/html/phpgroupware');
```

To:

```
define('PHPGW_SERVER_ROOT','/var/www/html/egroupware');
define('PHPGW_INCLUDE_ROOT','/var/www/html/egroupware');
```

Point your Browser to the URL

https://www.domain.com/egroupware/setup

Login to **Setup/Config Admin Login**

Click Edit Current Configuration

and change the content of the third field (Enter the location…) to: /egroupware

That's all…have fun!

5 Updating eGroupWare

5.1 When you should update?

The eGroupWare project releases the following types of releases: minor bug fix, major bug fix, security and new version. You should update immediately whenever **any** security release is announced. Security releases are officially announced when an external security researcher finds a problem and publishes it.

When the development team itself finds a security problem, the fix will be included in the next release but it is **not** announced on the mailing lists! This is to protect users who do not read the list very often, as it will be less likely that malicious user will find the exploit and use it on their own. If such a flaw is announced on the mailing list it needlessly provides malicious users with the knowledge to take advantage of the exploit.

You don't need to update eGroupWare when a release is a minor bug fix if you are not experiencing the symptoms of the bug. Minor bug fix releases don't include security fixes, and they normally only solve very specific problems.

A update to eGroupWare when a major bug fix or major version release is announced is generally recommended. These releases can include unannounced security fixes.

5.2 Updating the eGroupWare installation

Before you start to update your installation, make a backup from your eGroupWare files and he database.

1) Download the packages from our sourceforge[3] page.

2) Install the packages on your server:

   For RPM packages do the following:

   *[root@server tmp]# rpm –Uvh eGroupWare**

   For tar.gz packages go to your web server's root directory (above your eGroupWare installation):

   [root@server tmp]# cd /var/www/html
   [root@server html]# tar xzvf eGroupWare-x.xx.xxx-x.tar.gz

3 http://www.sf.net/projects/egroupware

For tar.bz2 packages go to your web server's root directory (above your eGroupWare installation):

[root@server tmp]# cd /var/www/html
[root@server html]# tar xjvf eGroupWare-x.xx.xxx-x.tar.bz2

It is possible to update from CVS. Update from CVS **ONLY** from the stable branch and not from the development branch!

[root@server tmp]# cd /var/www/html/egroupware
[root@server egroupware]# cvs update –r Version-1_0_0-branch -Pd

3) Login to Setup/Config Admin.
4) If necessary, eGroupWare will show you that you have to update your database tables.
5) Check for necessary updates in Step 4, Advanced Application Management.

5.3 Porting your settings to the new header.inc.php version

1) After update you will see the follow message:
   You need to port your settings to the new header.inc.php version.
2) Go to https://yourserver/egroupware/setup.
   - Scroll down in "Checking the eGroupWare Installation"
   - Confirm the check by pressing Continue to go to the Header Admin
3) Login with the correct username and password.
4) If necessary, change the settings.
5) Save the file.

6 Installation Instructions

6.1 Downloading the packages

You can download the packages from:
http://sourceforge.net/project/showfiles.php?group_id=78745

We provide the following packages at the Sourceforge download area:

*.tar.gz
*.tar.bz2
*.zip

These packages are signed with a gpg key for security reasons:

*.tar.gz.gpg
*.tar.bz2.gpg
*.zip.gpg

These packages work under Windows and offer a graphical installer:

egroupware*windows-installer.exe

These packages work under Linux and offer a graphical installer under X-Windows:

egroupware*linux-installer.bin

These RPMs work under Red Hat and most RPM-based distributions:

eGroupWare*noarch.rpm

The package **eGroupWare-all-apps*.noarch.rpm** contains all available packages.
The other packages provide all applications in separate packages.

6.2 Why are GPG-signed packages and md5sum necessary?

Sometimes hackers attack development servers to change the downloadable packages, and include trojan horses, sniffers, etc. in the packages. The signed packages validate the integrity of the project packages before you install and run the applications on your server.

6.2.1 Installing the GPG key for tar.gz.gpg, tar.bz2.gpg and zip.gpg

Install the GPG key with which the packages tar.gz.gpg, tar.bz2.gpg, zip.gpg, md5sum-eGroupWare-version.txt.asc and the RPM's are signed.

Under Linux you can use the following command to import the key so that you can validate the packages tar.gz.gpg, tar.bz2.gpg, zip.gpg and md5sum*.asc.

[root@server root]# gpg --keyserver blackhole.pca.dfn.de --recv-keys 0xD9B2A6F2

6.2.2 Verifying the GPG key

If you want to validate packages, you must trust the key. If you don't do this, you will receive an error that the key is not trusted every time.

List the available keys in your key ring. You must be able to see the imported key here:

[root@server root]# ***gpg --list-keys***
gpg: Warning: using insecure memory!
gpg: please see http://www.gnupg.org/faq.html *for more information*
/root/.gnupg/pubring.gpg
---
pub 1024D/D9B2A6F2 2002-12-22 Reiner Jung <r.jung@creativix.net>
sub 1024g/D08D986C 2002-12-22

Now edit the key with the key number **D9B2A6F2**

[root@server root]# gpg --edit-key D9B2A6F2
gpg (GnuPG) 1.0.7; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
gpg: Warning: using insecure memory!
gpg: please see http://www.gnupg.org/faq.html *for more information*
gpg: checking the trustdb
gpg: no ultimately trusted keys found

pub 1024D/D9B2A6F2 created: 2002-12-22 expires: never trust: -/-
sub 1024g/D08D986C created: 2002-12-22 expires: never
(1). Reiner Jung <r.jung@creativix.net>

You can (but don't have to) check the fingerprint of the key. The fingerprint of the key is:
BBFF 354E CA1F 051E 932D 70D5 0CC3 882C D9B2 A6F2

Command> fpr
pub 1024D/D9B2A6F2 2002-12-22 Reiner Jung <r.jung@creativix.net>
Fingerprint: BBFF 354E CA1F 051E 932D 70D5 0CC3 882C D9B2 A6F2

Now you can sign the key

Command>trust
pub 1024D/D9B2A6F2 created: 2002-12-22 expires: never trust: f/-
sub 1024g/D08D986C created: 2002-12-22 expires: never
(1). Reiner Jung <r.jung@creativix.net>

Please decide how far you trust this user to correctly
verify other users' keys (by looking at passports,
checking fingerprints from different sources...)?

1 = Don't know
2 = I do NOT trust
3 = I trust marginally
4 = I trust fully
5 = I trust ultimately
i = please show me more information
m = back to the main menu

Your decision? 5
Do you really want to set this key to ultimate trust? yes

pub 1024D/D9B2A6F2 created: 2002-12-22 expires: never trust: u/-
sub 1024g/D08D986C created: 2002-12-22 expires: never
(1). Reiner Jung <r.jung@creativix.net>
Please note that the shown key validity is not necessary correct
unless you restart the program.

Now you can check the key at the prompt with "check" or quit the session.

6.2.3 Installing the GPG key for the RPM packages

To import the key needed to validate the RPM packages, search for the key D9B2A6F2 on the following key server webpage : http://www.dfn-pca.de/eng/pgpkserv/

Click the link "D9B2A6F2." In the new window copy the full text, including the following lines:

----BEGIN PGP PUBLIC KEY BLOCK----
-----END PGP PUBLIC KEY BLOCK-----

Save the copied text to a file with the following name:

EGROUPWARE-GPG-KEY

Then import the key to your RPM key ring:

[user@server tmp]$ rpm --import EGROUPWARE-GPG-KEY

6.3 How do I validate packages?

If you want to check the **md5sum** of a package, perform the following steps (steps shown are for a Linux system):

Download the **md5sum-eGroupWare-version.txt.asc** file from the Sourceforge download page.

Validate the file **md5sum-eGroupWare-version.txt.asc**:

[user@server tmp]$ gpg --verify md5sum-eGroupWare-version.txt.asc

Find out the md5sum of the package:

[user@server tmp]$ md5sum eGroupWare-x.x.xx.xxx-x.tar.gz
41bee8f27d7a04fb1c3db80105a78d03 eGroupWare-x.x.xx.xxx-x.tar.gz

Open the md5sum file to see the original md5sum (the md5sum shown below is an example only):

user@server tmp]$ less md5sum-eGroupWare-x.x.xx.xxx-x.txt.asc

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

md5sum from file eGroupWare-x.x.xx.xxx.tar.gz is:
41bee8f27d7a04fb1c3db80105a78d03
- --

md5sum from file eGroupWare-x.x.xx.xxx.tar.bz2 is:
3c561e82996349d596540f476b9624f2
- --

md5sum from file eGroupWare-x.x.xx.xxx.zip is:
c3bb1f67ca143236e8603c6995e82db0
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.1 (GNU/Linux)

iD8DBQE/WM2wDMOILNmypvIRAm5GAJ0e6IlnellZU0quVQxWOP/pF+QGpwCgptbH
O02LpinLNqnr6epxt9vB9sw=
=OBcn
-----END PGP SIGNATURE-----

Here we see that the key in the md5sum file and the checksum test from the command line are the same, so the package was not changed after build.

To check the checksum from the tar.gz.gpg, tar.bz2.gpg or zip.gpg packages, type the following on the command line of your Linux system:

[user@server tmp]$ gpg --verify eGroupWare-x.x.xx.xxx-x.tar.gz.gpg

To check the checksum of the RPM package, type the following on the command line of your Linux system:

[user@server tmp]$ rpm --checksig eGroupWare-all-apps-x.x.xx.xxx-x.noarch.rpm

6.4 Installing the packages on your server

6.4.1 Installing an unsigned package on your server

To install an unsigned, non-RPM package, perform the following steps:

Change to your web server's document root (or wherever you want install the packages)

[user@server tmp]$ cd /var/www/html

Extract the package into this folder. If you have your package in the /tmp directory, you can install it with one of the following commands, depending on which package you have:

[user@server tmp]$ tar xzvf /tmp/eGroupWare-x.xx.xxx-x.tar.gz

[user@server tmp]$ tar xjvf /tmp/eGroupWare-x.xx.xxx-x.tar.bz2

[user@server tmp]$ unzip /tmp/eGroupWare-x.xx.xxx-x.zip

6.4.2 Installing a GPG-signed package on your server

To install a GPG-signed, non-RPM package, perform the following steps:

Detach your package from the GPG key:

[user@server tmp]$ gpg -o eGroupWare-X.XX.XXX-X.tar.gz -decrypt eGroupWare-X.XX.XXX-X.tar.gz.gpg

Change to your web server's document root (or wherever you want to install the packages)

[user@server tmp]$ cd /var/www/html

Extract the package into this folder. If you have your package in the /tmp directory, you can install it with one of the following commands, depending on which package you have:

[user@server html]$ tar xzvf /tmp/eGroupWare-x.x.xxx-x.tar.gz

[user@server tmp]$ tar xjvf /tmp/eGroupWare-x.xx.xxx-x.tar.bz2

[user@server tmp]$ unzip /tmp/eGroupWare-x.xx.xxx-x.zip

6.4.3 Install an RPM package on your server

To install a RPM package on your server, perform the following steps:

Check that the RPM is valid:

[user@server tmp]$ rpm --checksig /tmp/eGroupWare-x.x.xxx-x.noarch.rpm

Install the package:

[user@server tmp]$ rpm -ivh /tmp/eGroupWare-all-apps-x.x.xxx-x.noarch.rpm

If your web server root is **not** /var/www/html/ you can install the RPM to another path. To do this, use the following command.

[user@server tmp]$ rpm -ivh –prefix /your_new_server/eGroupWare-all-apps-x.x.xxx-x.noarch.rpm

6.4.4 Rebuilding the packages for other RPM paths

You can rebuild the RPM packages for SUSE LINUX. Download the file ***.src.rpm** and type

[user@server tmp]$ rpmbuild –-rebuild eGroupWare-x.xx.xxx-x.src.rpm

This will create a package with install path "/srv/www/htdocs" for you.
The package will be located for installation in /usr/src/packages/RPMS/noarch.

6.4.5 Install with Bitrock installer under Windows

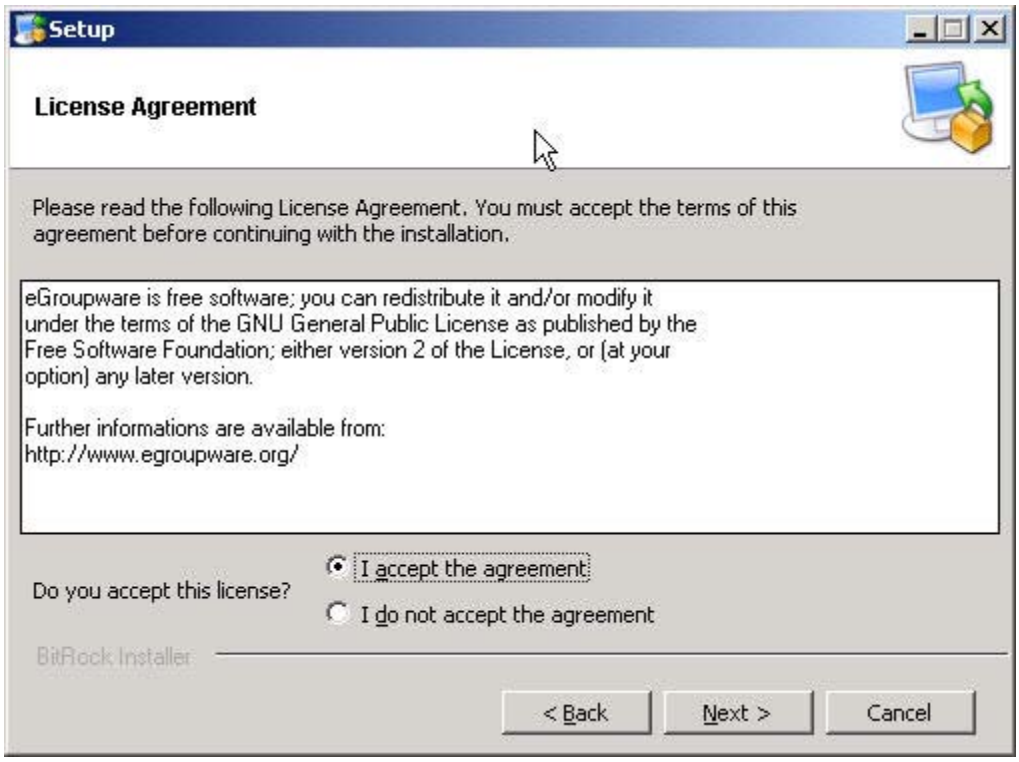
The installation with the graphical installer is very simple and can be done in 6 steps.

Klick the Windows installer executable to start the installation.

Select your language.

Click forward in the welcome screen.

You must accept the license agreement and click forward.



Choose the installation directory for your eGroupWare installation, as example f:\webapp

When the installation is done, you can view the Readme or finish the installation process.

6.4.6 Install with Bitrock installer under Linux

Bitrock installer can run under X-Windows or from a command line.

6.4.6.1 Use a GUI to install eGroupWare

Open a terminal window in your window manager to start the installer.

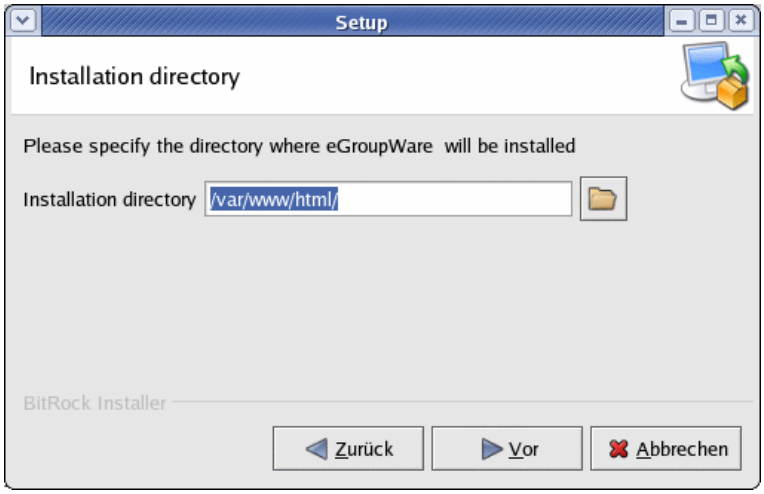
Change to the folder where you have downloaded the package, make the package executable and start the installation process.

[user@server tmp]$ chmod 700 egroupware-x-linux-installer.bin

[user@server tmp]$ ./egroupware-x-linux-installer.bin

The installation with the graphical installer is very simple and can be done in 7 steps.

Select your preferred language
Click forward in the welcome screen.
You must accept the license agreement and klick forward.
You can change the installation directory from /var/www/html to a other directory



When the installation is done, you can view the Readme or finish the installation process.
The Readme file includes some important information and is recommended reading.

6.4.6.2 Use the command line install eGroupWare

The installation process from the command line is nearly the same as from the GUI. You must make the package executable and execute the binary package. You will be see the same prompts as under the GUI installer

---

Welcome to the eGroupWare Setup Wizard

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Press [Enter] to continue :
The eGroupWare software is distributed under the Terms of
GPL and LGPL.
It is free of Charge
Redistribution is allowed.

Do you accept this license? [Y/n]: n

6.4.7 Installing from CVS

To install the packages from the CVS repository, perform the following steps:

Change to your web server's document root (or wherever you want to install the packages):
:

[root@server tmp]# cd /var/www/html

[root@server html]# cvs –d:pserver:anonymous@cvs.sourceforge.net:
/cvsroot/egroupware login

[root@server html]# cvs –z3 –d:pserver:anonymous@cvs.sourceforge.net:
/cvsroot/egroupware co egroupware
(The above should be all on one line, i.e. you should have …sourceforge.net:/cvsroot/eg…)

[root@server html]# cd egroupware

[root@server egroupware]# cvs co all
[root@server egroupware]# cvs update –Pd

A good introduction covering CVS usage in Open Source Development can found in the book Open Source Development with CVS[4]

4 http://cvsbook.red-bean.com/OSDevWithCVS_3E.pdf

7 Basic Server Security

7.1 Partitioning the filesystem

A standard *nix installation often consists of only 2 partitions, **/boot** and **/**. This is a security and availability risk for your server. There are several different exploits and attacks available where a hacker can, for instance, use the /tmp file system to compile an exploit or run a symlink attack, or an attacker can shut down your server by flooding the hard drive with logs or mails. To be prepared again these kinds of attacks you should select a partitioning scheme that uses more then 2 partitions.

A good partition scheme should have an /etc/fstab file that looks like the following example:

```
LABEL=/                 /                       ext3    defaults        1 1
LABEL=/boot             /boot                   ext3    defaults        1 2
LABEL=/home             /home                   ext3    defaults        1 2
LABEL=/opt              /opt                    ext3    defaults        1 2
LABEL=/usr              /usr                    ext3    defaults        1 2
LABEL=/var              /var                    ext3    defaults        1 2
LABEL=/var/www/files    /var/www/files          ext3    defaults        1 2
LABEL=/var/log          /var/log                ext3    defaults        1 2
LABEL=/var/mail         /var/mail               ext3    defaults        1 2
LABEL=/tmp              /tmp                    ext2    auto,noexec,nosuid,rw   1 2
/dev/hda11              swap                    swap    defaults        0 0
```

If you also host “normal” user accounts on the same server, use the mount options usrquota and grpquota. This prevents users from filling the home directories to capacity

7.2 The server platform

There are many ways you can secure your server platform. The most important security measure you can perform is to keep your installation up-to-date. Consider subscribing to the egroupware-announcement@lists.sourceforge.net mailing list. This is where we publish new releases as well as necessary security updates for eGroupWare.

7.2.1 Checking your server for running services and open ports

An open port indicates that your server is offering a service to the public. This could be a Fileserver, DNS Server, Telnet server, X server or one of many other services. More open ports provide an attacker with more ways that an exploit can gain access to your running services to gain control. You server should only have the ports open and services available which are necessary to run eGroupWare. If you need other open ports that are not necessary for eGroupWare, then you should secure your installation with a firewall or with TCP wrappers. If it's possible, only allow services to run on your eGroupWare server that have **Secure Socket Layer** (SSL) enabled.

7.2.1.1 Ports which the eGroupWare server needs to run

Ports which are needed are:

Web server Port:	HTTP/80
Web server SSL Port:	HTTPS/443
Remote Administration, Secure Shell:	SSH/22

If you must run an E-Mail server on the same machine, then you will need a few more ports open. If you can run your E-Mail server on a separate machine, then please do so. You'll need these extra ports open for an E-Mail server to run:

Email Server MTA:	SMTP/25
Email Server MTA:	SMTPS/465

To pick up the E-Mail from your server with a client program (such as the eGroupWare clients), you need a POP3 or IMAP daemon which will require at least one of following ports open:

IMAP server:	IMAP/143
IMAP server SSL:	IMAPS/993
POP-3:	POP-3/110
POP-3 over SSL:	POP-3/995

If you block ports with a firewall, please remember that you will need to allow certain outbound traffic. This can include NTP, DNS lookups, etc.

Conclusion:

Minimum necessary open ports (non-SSL):	22, 80, 443
Maximum necessary open ports (including E-Mail server):	22, 25, 80, 110, 143, 443, 465, 993, 995
Recommended minimum (SSL only, no E-Mail server):	22, 443
Recommended maximum (SSL only, E-Mail server):	22, 25, 443, 993, 995

7.2.1.2 The portscanner

There are several tools available that will allow you to check your installation for open ports. One that is available under both *NIX and Windows is Nmap, which can be found at: http://www.insecure.org/nmap.

Install Nmap on your machine and check your server for open ports.

7.2.1.3 Output from a portscanner

Here is example output from a Nmap scan against a server. Nmap shows you the ports which are open to connect to on this server.

```
[root@server root]# nmap -sV  yourserver.com
Starting nmap 3.45 ( http://www.insecure.org/nmap/ ) at 2003-09-17 00:48 CEST
Interesting ports on xxx.xxx.xx.xxx:
(The 1651 ports scanned but not shown below are in state: closed)
PORT    STATE    SERVICE     VERSION
22/tcp  open     ssh         OpenSSH 3.1p1 (protocol 2.0)
80/tcp  open     http        Apache httpd 1.3.27 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.12
                             OpenSSL/0.9.6b PHP/4.1.2 mod_perl/1.26)
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
443/tcp open     ssl         OpenSSL
```

Nmap run completed -- 1 IP address (1 host up) scanned in 23.000 seconds

7.2.1.4 Disabling unneeded services/servers

If Nmap found services running on your server that you do not need, stop them. After you restart the service should not automatically start again.

On a Red Hat installation you can use the following commands to stop and disable a service:

```
[root@server home]# service name_from_the_service stop

[root@server home]# chkconfig –level 345 name_from_the_service off
```

On a Debian-based installation you can use the following tools:

```
Server:~# /etc/init.d/ name_from_the_service stop

Server:~# rcconf
```

On a SUSE-based installation you can use the following commands:

Server:~# /etc/init.d/name_from_the_service stop

Server:~# chkconfig name_from_the_service off

7.2.2 Uninstalling unneeded software on your server

Most operating system distributions by default install a lot of software which is not necessary. For security reasons you should delete this software from your server. Unneeded software often includes things like ftp clients and wget. If you are not going to be compiling anything from source, you should also remove gcc, header files, and source files.

To check what packages are installed on a RPM-based Linux distribution, do the following:

[root@server home]# for i in `rpm –qa`; do rpm –qi $i >> rpm_packages; done

[root@server home]# less rpm_packages

Delete all packages which you don't need:

[root@server home]# rpm –e package

To check what packages are installed on a **Debian-**based Linux, Debian offers many tools. In example;

Server:~# aptitude

7.2.3 Check for rootkits on your server

For Linux/*nix there are two nice open source products on the market to detect rootkits. It is strongly recommended that you install a rootkit checker on your server. You can choose between chkrootkit[5] and rootkit hunter[6].

7.2.3.1 Local check for signs of a rootkit with chkrootkit

Chkrootkit is a tool to locally check for signs of a rootkit. Chkrootkit has been tested on: Linux 2.0.x, 2.2.x and 2.4.x, FreeBSD 2.2.x, 3.x, 4.x and 5.x, OpenBSD 2.x and 3.x., NetBSD 1.5.2, Solaris 2.5.1, 2.6 and 8.0, HP-UX 11, True64 and BSDI. It contains:

- chkrootkit: A shell script that checks your system binaries for rootkit modification. The following are checked:

  aliens asp bindshell lkm rexedcs sniffer wted w55808 scalper slapper z2 amd basename biff chfn chsh cron date du dirname echo egrep env find fingerd gpm grep hdparm su ifconfig inetd inetdconf init identd killall ldsopreload login ls lsof mail mingetty netstat named passwd pidof pop2 pop3 ps pstree rpcinfo rlogind rshd slogin sendmail sshd syslogd tar tcpd tcpdump top telnetd timed traceroute vdir w write

- ifpromisc.c: checks if the network interface is in promiscuous mode.
- chklastlog.c: checks for lastlog deletions.
- chkwtmp.c: checks for wtmp deletions.
- check_wtmpx.c: checks for wtmpx deletions. (Solaris only)
- chkproc.c: checks for signs of LKM trojans.
- chkdirs.c: checks for signs of LKM trojans.
- strings.c: quick and dirty strings replacement

You can download chkrootkit as a compiled RPM package or as a tar.gz package by clicking one of the following links (hold Ctrl as you click):

chkrootkit.tar.gz[7]
chkrootkit RPM[8]

5 http://www.chkrootkit.org
6 http://www.rootkit.nl
7 http://www.chkrootkit.org
8 http://www.expl0it.de/rpms/security/chkrootkit/

7.2.3.2 Chkrootkit sample snippet

Checking `timed'... not found
Checking `traceroute'... not infected
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for HiDrootkit's default dir... nothing found
Searching for t0rn's default files and dirs... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for Lion Worm default files and dirs... nothing found
Searching for RSHA's default files and dir... nothing found
Searching for RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found

7.2.3.3 Installing the chkrootkit RPM

The chkrootkit RPM should run with all RPM-based distributions.
Download it from the address above and install it as follows:

[root@server tmp]# rpm –ivh chkrootkit-x.xx-x.i386.rpm

After installation, you can modify the chkrootkit_cronfile to better suit your needs. This step is not necessary, but makes your report more unique.

[root@server tmp]# vi /etc/cron.daily/chkrootkit_cronfile

```
#!/bin/sh
cd /usr/bin ./chkrootkit 2> /dev/null | mail –s “chkrootkit output” root

Change the following values:
“chkrootkit output” to “chkrootkit myserver output” root
          to
your_email_adress@yourserver.com
```

7.2.3.4 Installing chkrootkit from the tar.gz file

Unpack and install Chkrootkit

[root@server tmp]# cp chkrootkit.tar.gz /usr/local; rm chkrootkit.tar.gz

[root@server tpm]# cd /usr/local/

[root@server local]# tar xzvf chkrootkit.tar.gz

[root@server local]# mv chkrootkit-x.xx chkrootkit

[root@server local]# chown –R root.root chkrootkit
[root@server chkrootkit]# cd chkrootkit

[root@server chkrootkit]# make sense

To make chkrootkit send you the report you have two possibilities: create a chkrootkit_cronfile or add a line to the crontab file.

To create a chkrootkit_cronfile:

[root@server cron.daily]# vi chkrootkit_cronfile

```
#!/bin/sh
cd /usr/local/chkrootkit ./chkrootkit 2> /dev/null | mail –s "chkrootkit
myserver output" your_email_adress
```

Alternatively, extend the crontab file with the following line:

```
0 1 * * *   root    (cd /usr/local/chkrootkit; ./chkrootkit 2>&1 | mail –
s  "chkrootkit output" your_email_adress)
```

Now chkrootkit will send you a report to the address above.

7.2.4 Secure server administration

If you want to administrate your server securely, use SSH (secure shell). With SSH, all connections are encrypted, whereas with protocols like telnet and ftp, the user accounts and passwords are transmitted unencrypted (in clear text format). The transfer of the passwords and account information is easy for an attacker to sniff if it is in clear text. With the sniffed passwords, a hacker can login to your account.

If possible, use only SSHv2 connections and never use SSHv1 connections. SSHv1 has a known flaw that can allow the encrypted information to be deciphered by an attacker. Also, don't use your root account to log in to the remote server. Connect to the remote server with a normal user account and use su or sudo for administration tasks on the server.

7.2.4.1 Connecting to your server over a secure session

If your server supports SHH connections, then it is easy to administrate it remotely. You only have to connect to the server with you SSH client.

The first time you connect to any particular server with SSH, you will receive a warning like the following. You must agree to the warning with yes to continue to log in to the server.

[user@client home]$ ssh yourserver
The authenticity of host 'yourserver (100.178.76.207)' can't be established.
RSA key fingerprint is 7e:8e:55:8b:49:57:5d:41:40:ab:93:64:18:af:60:ea.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'yourserver' (RSA) to the list of known hosts.

Connect to your server for remote administration:
[user@client home]$ ssh yourserver

Copy files to your server with secure copy (scp):
[user@client home]$ scp yourfile.txt yourserver:/home/

You can also use sftp to work with a "secure ftp client":
[user@client home]$ sftp yourserver

In some installations, the sftp function is disabled by default (for example, in some versions of Debian). If you want enable it, you must add the following line to your **sshd_config** on your server.

On a Debian system add the following line:
subsystem sftp /usr/lib/sftp-server

On a RedHat system add the following line:
subsystem sftp /usr/libexec/openssh/sftp-server

7.2.4.2 Working with SSH Key Pairs

Using SSH Key Pairs has two advantages. The first is that you don't need to type your password every time you connect to the server, and the second is that it is more secure. When you use key pairs you can permit the usage of authenticating with a different password than that of your account on the server.

You need a separate key pair for every user you want to connect to the server with.

7.2.4.2.1 Creating a secure shell key pair

You must create the ssh key pair on the client side as follows:

[user@client home]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /user/.ssh/id_dsa.
Your public key has been saved in /user/.ssh/id_dsa.pub.
The key fingerprint is:
f0:00:f7:95:e9:73:37:11:aa:e8:06:3e:60:9e:0d:25 user@yourserver

7.2.4.2.2 Copying your public key to the server

You must copy your new public key (*.pub) from your local client to the server:

[user@client home]$ scp .ssh/id_dsa.pub useratserver@yourserver:/home/yoursername/

Install the public key on your server:

[user@client home]$ ssh yourserver
[user@server home]$ cat id_dsa.pub >> .ssh/authorized_keys
[user@client home]$ chmod 600 .ssh/authoritzed_keys

Now, if you connect to the server, the server asks you for the password which you typed when you created the SSH key pair. If you don't want type it every time when you connect to the server, you can use ***ssh-add****.*

7.2.4.2.3 The ssh-add tool

If you connect to your server (or different servers) frequently, you can use the ssh-add tool to store the password from your ssh key. Then you can just type your password once and it is stored for you permanently:

[user@client home]$ ssh-add
Enter passphrase for /home/youruser/.ssh/id.dsa:
Identify added: /home/youruser/.ssh/id.dsa (/home/youruser/.ssh/id.dsa)

7.2.4.2.4 Securing your SSH client

There is one important line in the configuration file from the SSH client. The make sure the following line exists in your **ssh_config** file:

Protocol 2

This allows your clients connections with the version 2 of the SSH protocol only.

7.2.4.2.5 Securing your SSHD

For your SSH daemon you can use the following values to make it more secure:

```
Protocol 2
PermitRootLogin no
PubKeyAuthentication yes
PasswordAuthentication no
PermitEmptyPassword no
```

7.2.5 Installing software to monitor your server logs

Analyzing your log files is a must for every administrator. When you don't monitor your log files, you have no chance of seeing security problems or anomalies. There are several products on the market that can help you to monitor your log files:

logcheck [9]
logwatch [10]
logsurfer [11]

Logcheck is recommended. Logcheck will work under Linux, BSD, Sun, and HP-UX. It is easy to install and make clear reports. To install logcheck type the following from the logcheck root after you have un-tared the file:

[root@server logcheck-1.1.1]# make linux

9 http://sourceforge.net/project/showfiles.php?group_id=80573&release_id=161261
10 http://www2.logwatch.org:81/tabs/download/
11 http://www.cert.dfn.de/eng/logsurf/

To run it automatically, you must add a line to your crontab file. Under RedHat, it is /etc/crontab. Open the file (you may have to open it by typing in "crontab –e") and add the following line:

```
00 * * * * root /bin/sh /usr/local/etc/logcheck.sh
```

Edit the logcheck shell script to add the recipient to the log report. The recipient is the value of the SYSADMIN variable in the script.

[root@egroupware logcheck-1.1.1]# vi /usr/local/etc/logcheck.sh

To receive more detailed reports, advanced users can also edit the following files:

logcheck.violations
logcheck.violations.ignore
logcheck.hacking
logcheck.ignore

7.2.6 Intrusion detection environment

Install an intrusion detection environment to keep check of your system files' integrity and to detect changes on your server.

There are several solutions available for *nix based systems. Osiris work under *nix and Windows.

AIDE [12]
Osiris[13]
Tripwire [14]
Samhain [15]

From the software above, AIDE is the easiest to set up.

7.2.6.1 Installing AIDE

Most distributions have AIDE included and you can install it with a standard tool like RPM or apt-get. AIDE depends on the mhash package, which you must install as well. When no package is available for your platform, you must compile it yourself with

./configure
make
make install

12 http://sourceforge.net/projects/aide/
13 http://osiris.shmoo.com
14 http://www.tripwire.org/
15 http://www.samhain-labs.org/

7.2.6.2 The AIDE configuration file aide.conf

You must configure the aide.conf file so that all important files from your server are checked and to reduce false alarms.

Store /etc/aide.conf, /usr/sbin/aide and /var/lib/aide/aide.db.gz in a secure location, e.g. on separate read-only media (such as CD-ROM). Alternatively, keep MD5 fingerprints or GPG signatures of those files in a secure location, so you have a means to verify that nobody has modified these files.

```
# Example configuration file for AIDE.
@@define DBDIR /var/lib/aide

# The location of the database to be read.
database=file:/mnt/floppy/aide.db.gz

# The location of the database to be written.
database_out=file:@@{DBDIR}/aide.db.new.gz

# Whether to gzip the output to the database
gzip_dbout=yes

# Default.
verbose=5

report_url=file:/var/log/aide.log
report_url=stdout

# These are the default rules.
#
#p:      permissions
#i:      inode:
#n:      number of links
#u:      user
#g:      group
#s:      size
#b:      block count
#m:     mtime
#a:      atime
#c:      ctime
#S:      check for growing size
#md5:    md5 checksum
#sha1:   sha1 checksum
#rmd160: rmd160 checksum
#tiger:  tiger checksum
#haval:  haval checksum
```

```
#gost:   gost checksum
#crc32:  crc32 checksum
#R:      p+i+n+u+g+s+m+c+md5
#L:      p+i+n+u+g
#E:      Empty group
#>:      Growing logfile p+u+g+i+n+S

# You can create custom rules like this.
NORMAL = R+b+sha1
DIR = p+i+n+u+g

# Next decide what directories/files you want in the database.

/boot   NORMAL
/bin    NORMAL
/sbin   NORMAL
/lib    NORMAL
/opt    NORMAL
/usr    NORMAL
/root   NORMAL

# Check only permissions, inode, user and group for /etc, but
# cover some important files closely.
/etc    p+i+u+g
!/etc/mtab
/etc/exports  NORMAL
/etc/fstab    NORMAL
/etc/passwd   NORMAL
/etc/group    NORMAL
/etc/gshadow  NORMAL
/etc/shadow   NORMAL
```

Run "aide --init" to build the initial database.

[root@server root]# /mnt/floppy/aide –init

Copy /var/lib/aide/aide.db.new.gz to the secure location

[root@server root]# cp /var/lib/aide/aide.db.new.gz /mnt/floppy/var/lib/aide/aide.db.gz

Check your system for inconsistencies with the AIDE database. Prior to running a check manually, ensure that the AIDE binary and database have not been modified without your knowledge.

[root@server root]# /mnt/floppy/aide --check

7.2.6.3 Creating a cronjob file to run AIDE automatically

This file is included in the Debian AIDE package, so if you have installed AIDE from a deb package you don't need to create this file yourself. The file shown below is an example file which has been modified for RedHat / Fedora Linux. When you want create a cron file for another distribution, you will probably need to change the paths.

```
#!/bin/sh

PATH="/bin:/usr/sbin:/usr/bin"
LOGFILE="/var/log/aide.log"
CONFFILE="/etc/aide.conf"
ERRORLOG="/var/log/error.log"

[ -f /usr/sbin/aide ] || exit 0

MAILTO=”yourusername”
DATABASE=`grep "^database=file:/" $CONFFILE | head -1 | cut -d: -f2`
LINES=”1000”
FQDN=`hostname -f`
DATE=`date +"at %X on %x"`

[ -z "$MAILTO" ] && MAILTO="root"

if [ ! -f $DATABASE ]; then
          (
          echo "Fatal error: The AIDE database does not exist!"
          echo "This may mean you haven't created it, or it may mean that
someone has removed it."
          ) | /bin/mail -s "Daily AIDE report for $FQDN" $MAILTO
          exit 0
fi

aide --check >$LOGFILE 2>$ERRORLOG

(cat << EOF;
This is an automated report generated by the Advanced Intrusion Detection
Environment on $FQDN ${DATE}.

EOF
if [ -s $LOGFILE ]; then
          loglines=`wc -l $LOGFILE | awk '{ print $1 }'`
          if [ ${loglines:=0} -gt $LINES ]; then
                    echo
                    echo "TRUNCATED (!) output of the daily AIDE run:"
```

```
                    echo "Output is $loglines lines, truncated to
$LINES."
                    head -$LINES $LOGFILE
                    echo "The full output can be found in $LOGFILE."
          else
                    echo "Output of the daily AIDE run:"
                    cat $LOGFILE
          fi
else
          echo "AIDE detected no changes."
fi
if [ -s $ERRORLOG ]; then
          errorlines=`wc -l $ERRORLOG | awk '{ print $1 }'`
          if [ ${errorlines:=0} -gt $LINES ]; then
                    echo "TRUNCATED (!) output of errors produced:"
                    echo "Error output is $errorlines lines, truncated
to $LINES."
                    head -$LINES $ERRORLOG
                    echo "The full output can be found in $ERRORLOG."
          else
                    echo "Errors produced:"
                    cat $ERRORLOG
          fi
else
          echo "AIDE produced no errors."
fi
) | /bin/mail -s "Daily AIDE report for $FQDN" $MAILTO
```

It is not recommended that you run automated AIDE check without verifying AIDE yourself frequently. In addition to that, AIDE does not implement any password or encryption protection for its own files.

7.2.6.4 Sample AIDE report

The report which AIDE creates shows you all changes on your file system. Please compare the report with the changes you have made (i.e. installing an update or changing the configuration of your server).

This is an automated report generated by the Advanced Intrusion Detection
Environment on egroupware at 05:27:16 PM on 02/14/2004.

Output of the daily AIDE run:
AIDE found differences between database and filesystem!!
Start timestamp: 2004-02-14 17:27:16
Summary:
Total number of files=34691,added files=2,removed files=0,changed files=5

Added files:
added:/etc/cron.daily/aide
added:/var/log/error.log
Changed files:
changed:/etc/aide.conf
changed:/root
changed:/root/.viminfo
changed:/root/.bash_history
changed:/root/chkrootkit-0.44-1.i386.rpm
Detailed information about changes:

File: /etc/aide.conf
Inode : 89090 , 89173

Directory: /root
Mtime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12
Ctime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12

File: /root/.viminfo
Size : 6683 , 6513
Mtime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12
Ctime : 2004-02-14 16:35:58 , 2004-02-14 17:27:12
Inode : 111362 , 111363
MD5 : UM0erzXMWPEdiCgKV/t91g== , l9E0UBQu7PKTCJiS3b2Fzw==
SHA1 : jNlzWrSY/Q4zk3Rd7dnpyth2a0Y= , R1wFnTg2scWSaRnn47zcZ+syS3E=

File: /root/.bash_history
Size : 14824 , 14872
Mtime : 2004-02-14 16:16:30 , 2004-02-14 16:48:32
Ctime : 2004-02-14 16:16:30 , 2004-02-14 16:48:32

MD5 : zlVCx+39n8XLd3/ip757vA== , nCs18yzJdwDD/BfsUssuhQ==

SHA1 : Al8brD3i+B6P2RMxpn6IaC+I5fE= , bWBEjLA0Hnt6XXTszkzKi8gaTZQ=

File: /root/chkrootkit-0.43-1.i386.rpm

Permissions: -rw-r--r-- , -rw-r-----

Ctime : 2004-01-26 13:43:35 , 2004-02-14 16:51:06

AIDE produced no errors.

7.2.6.5 Creating a new database after changes

After your report is verified you must create a new database and save the database at the secure location. Run the update from your database after every report which you have verified!

[root@server root]# /mnt/floppy/aide --init

[root@server root]# cp /var/lib/aide/aide.db.new.gz /mnt/floppy/var/lib/aide/aide.db.gz

7.2.7 Daemon security

Run your necessary daemons in a chroot environment under *nix.

Use TCP Wrappers or xinetd to secure your daemons.

7.2.8 Firewall

Activate a firewall on your eGroupWare server to protect your installation. Some ports must be open but with a firewall (using, for instance, IPTABLES), you can protect your system again spoofing, ping flooding, and various other attacks.

7.2.8.1 Planing the firewall

The first thing you should do is decide which services you need. The ports used by these services will need to be allowed in your firewall script. Create a simple table in which you fill the services which must run. We do it here for an example eGroupWare installation

Protocol	Port	Description	Ingoing	Outgoing
HTTP	80	This protocoll we need to connect to eGW	✔	✔
HTTPS	443	Same as above		✔
SMTP	25	Run a internal Mailserver and must send mail	✔	✔
SMTPS	465	Same as above	✔	✔
IMAP	143	We allow only connetions to external IMAP		✔
IMAPS	993	We allow only connetions to external IMAPS		✔
POP3	995	We allow only connetions to external POP3		✔
DNS	53	We allow only connetions to external POP3S		✔
SSH	22	We must have console access	✔	
NTP	37	Network Time Protokoll, for server time		✔
CVS	2401	We want update our eGW with CVS		✔
RedHat Network	443	We use RedHat Network		✔

7.2.8.2 How create the firewall rules

There are many possibilities for creating a rule set for your IPTABLES-based firewall. Many people use a simple editor to create firewall rules or type them directly on the command line. I personally use VIM to write firewall rules; others use ed, mc, joe, or emacs.

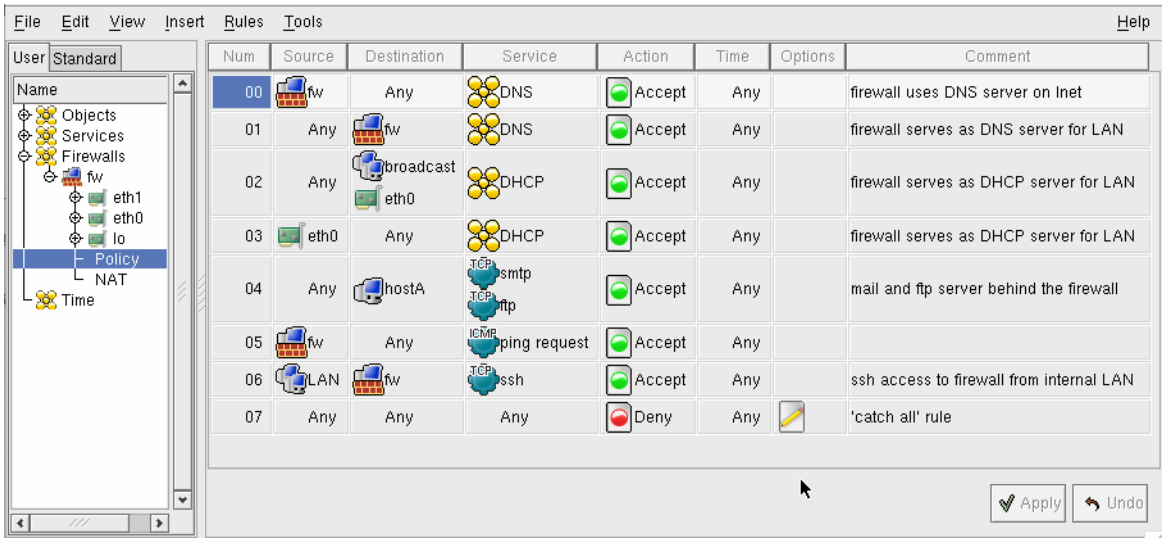
Shown here are two other solutions that can be used to create a firewall rule set. Many more are available, and can easily be found by searching on the Internet.

One of the other methods for creating an iptables-based firewall rule set is to use shorewall [16].
The Shoreline Firewall, more commonly known as "Shorewall", is a high-level tool for configuring Netfilter. You describe your firewall/gateway requirements using entries in a set of configuration files. Shorewall reads those configuration files and with the help of the iptables utility Shorewall configures Netfilter to match your

16 http://www.shorewall.net/

requirements.

When you prefer to use a graphical tool to write your rulesets, then you can use firewall builder [17].
Firewall Builder is multi-platform firewall configuration and management tool. It consists of a GUI and set of policy compilers for various firewall platforms. Firewall Builder uses object-oriented approach, which helps administrators maintain a database of network objects and allows policy editing using simple drag-and-drop operations.



7.2.8.3 Example firewall script

Based on the information in the table we designed in section 7.2.8.1, a working firewall script for a RedHat/Fedora server is shown below.

You must set the value for your OWN_IP_ADDRESS in this script ! Don't forget this **or you will be blocked !**

```
#!/bin/sh

IPTABLES="/sbin/iptables"
MODPROBE="/sbin/modprobe"

NETWORK_DEVICE="eth0"
OWN_IP_ADDR="SET_YOUR_IP_ADDRESS_HERE"
LOOPBACK="lo"

THE_SOURCEFORGE_CVS_SERVER_IP_ADDRESS="66.35.250.207"
IMAP_SERVER_ADDRESS_EXTERN="x.x.x.x"
POP_SERVER_ADDRESS="x.x.x.x"
NTP_SERVER_1_ADDRESS=`cat /etc/ntp.conf | grep ^server | cut -d " " -f 2
| head -n 1`
```

17 http://www.fwbuilder.org/

```
NTP_SERVER_2_ADDRESS=`cat /etc/ntp.conf | grep ^server | cut -d " " -f 2
| tail -n 1`
REDHAT_NETWORK_IP_ADDRESS="209.132.177.100"

PRIVAT_PORTS="1:1023"
NON_PRIVAT_PORTS="1024:65535"

$MODPROBE ip_tables

# Ignore ping to broadcast address
    echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

# Deactivate source routing
    for i in /proc/sys/net/ipv4/conf/*/accept_source_route; do
      echo 0 > $i
    done

# Enable TCP-SYN cookies
    echo 1 > /proc/sys/net/ipv4/tcp_syncookies

# Drop ICMP-redirect
    for i in /proc/sys/net/ipv4/conf/*/accept_redirects; do
      echo 0 > $i
    done

# Don't send ICMP-redirects
    for i in /proc/sys/net/ipv4/conf/*/send_redirects; do
      echo 0 > $i
    done

# Log packages with not possible addresses
    for i in /proc/sys/net/ipv4/conf/*/log_martians; do
      echo 1 > $i
    done

# Ignore packages when response should send over other interface
   for i in /proc/sys/net/ipv4/conf/*/rp_filter; do
      echo 1 > $i
    done

# Delete all existing chains
  $IPTABLES --flush
  $IPTABLES -t nat --flush
  $IPTABLES -t mangle --flush
```

```
# Loopback Device
  $IPTABLES -A INPUT -i $LOOPBACK -j ACCEPT
  $IPTABLES -A OUTPUT -o $LOOPBACK -j ACCEPT

# As standard policy, we drop all packages
  $IPTABLES --policy INPUT DROP
  $IPTABLES --policy OUTPUT DROP
  $IPTABLES --policy FORWARD DROP

# Delete User Chains
  $IPTABLES --delete-chain
  $IPTABLES -t nat --delete-chain
  $IPTABLES -t mangle --delete-chain

# accept packets that belong to sessions that have previously been proven
ok:
  $IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
  $IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

  $IPTABLES -A INPUT -m state --state INVALID -j LOG --log-prefix
  "INVALID input: "

  $IPTABLES -A INPUT -m state --state INVALID -j DROP

  $IPTABLES -A OUTPUT -m state --state INVALID -j LOG --log-prefix
  "INVALID output: "

  $IPTABLES -A OUTPUT -m state --state INVALID -j DROP

# SCAN PROTECTION for the server
# ALL BITS DELETED
  $IPTABLES -A INPUT -p TCP --tcp-flags ALL NONE -j DROP

# SYN and FIN set together
  $IPTABLES -A INPUT -p TCP --tcp-flags SYN,FIN SYN,FIN -j DROP

# SYN and RST set together
  $IPTABLES -A INPUT -p TCP --tcp-flags SYN,RST SYN,RST -j DROP

# FIN and RST set together
  $IPTABLES -A INPUT -p TCP --tcp-flags FIN,RST FIN,RST -j DROP

# FIN and no needed ACK
  $IPTABLES -A INPUT -p TCP --tcp-flags ACK,FIN FIN -j DROP
```

```
# PSH and no needed ACK
  $IPTABLES -A INPUT -p TCP --tcp-flags ACK,PSH PSH -j DROP

# URG and no needed ACK
  $IPTABLES -A INPUT -p TCP --tcp-flags ACK,URG URG -j DROP

# ICMP Controll and Status Messages

# Log and Drop icmp fragmentet packages
   $IPTABLES -A INPUT -i $NETWORK_DEVICE --fragment \
                    -p icmp -m limit --limit 2/s

  $IPTABLES -A INPUT --fragment -p icmp -j DROP

  $IPTABLES -A INPUT -i $NETWORK_DEVICE -p icmp --icmp-type \
                    source-quench -d $OWN_IP_ADDR -j ACCEPT

  $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p icmp \
                    -s $OWN_IP_ADDR --icmp-type source-quench -j ACCEPT

  $IPTABLES -A INPUT -i $NETWORK_DEVICE -p icmp --icmp-type \
                    parameter-problem -d $OWN_IP_ADDR -j ACCEPT

  $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p icmp -s $OWN_IP_ADDR \
                    --icmp-type parameter-problem -j ACCEPT

  $IPTABLES -A INPUT -i $NETWORK_DEVICE -p icmp --icmp-type \
                    destination-unreachable -d $OWN_IP_ADDR -j ACCEPT

  $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p icmp -s $OWN_IP_ADDR \
                    --icmp-type destination-unreachable -j DROP



  $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p icmp -s $OWN_IP_ADDR \
                    --icmp-type fragmentation-needed -j ACCEPT

# Allow traceroute to our server
    $IPTABLES -A INPUT -i $NETWORK_DEVICE -p icmp \
                    --icmp-type time-exceeded -d $OWN_IP_ADDR -j ACCEPT

# Allow ping to our server
    $IPTABLES -A INPUT -i $NETWORK_DEVICE -p icmp \
                    --icmp-type echo-request -d $OWN_IP_ADDR \
                    -m limit --limit 1/s -j ACCEPT
```

```
# Allow ping from our server to a other destination
    $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p icmp \
                    -s $OWN_IP_ADDR --icmp-type echo-request -j ACCEPT

# HTTP server
    $IPTABLES -A INPUT -i $NETWORK_DEVICE  -p TCP \
                    --dport http --sport $NON_PRIVAT_PORTS \
                    -m state --state NEW -j ACCEPT

    $IPTABLES -A INPUT -i $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS --dport https \
                    -m state --state NEW -j ACCEPT

   # We need outgooing http for news feeds and comics
     $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS --dport http \
                    -m state --state NEW -j ACCEPT

# SMTP Server
    $IPTABLES -A INPUT -i $NETWORK_DEVICE  -p TCP \
                    --dport smtp -m state --state NEW -j ACCEPT

     $IPTABLES -A INPUT -i $NETWORK_DEVICE -p TCP \
                    --dport smtps -m state --state NEW -j ACCEPT

     $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p TCP --dport smtp \
                    -m state --state NEW -j ACCEPT

     $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p TCP --dport smtps \
          -m state --state NEW -j ACCEPT


# IMAP Server
    $IPTABLES -A INPUT -i $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS --dport imap \
                    -m state --state NEW -j ACCEPT

    $IPTABLES -A INPUT -i $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS --dport imaps \
                    -m state --state NEW -j ACCEPT

    $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS -d
                    $IMAP_SERVER_ADDRESS_EXTERN --dport \
```

```
                    imap -m state --state NEW -j ACCEPT

  $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS \
                    -d $IMAP_SERVER_ADDRESS_EXTERN \
                    --dport imaps -m state --state NEW -j ACCEPT
# POP Server
   $IPTABLES -A INPUT -i $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS --dport pop3 \
                    -m state --state NEW -j ACCEPT

   $IPTABLES -A INPUT -i $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS --dport pop3s \
                    -m state --state NEW -j ACCEPT

   $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS \
                    -d $POP_SERVER_ADDRESS --dport pop3 \
                    -m state --state NEW -j ACCEPT

   $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS \
                    -d $POP_SERVER_ADDRESS --dport pop3s \
                    -m state --state NEW -j ACCEPT

# DNS Server
  $IPTABLES -A INPUT -i $NETWORK_DEVICE -p TCP \
                    --dport domain -m state --state NEW -j ACCEPT

  $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p UDP \
                    --dport domain -m state --state NEW -j ACCEPT

  $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p TCP \
                    --sport $NON_PRIVAT_PORTS --dport domain \
                    -m state --state NEW -j ACCEPT

  $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p UDP \
                    --sport $NON_PRIVAT_PORTS --dport domain \
                    -m state --state NEW -j ACCEPT

# NTP Server
  for NTP_SERVER in $NTP_SERVER_1_ADDRESS $NTP_SERVER_2_ADDRESS ; do
          $IPTABLES -A OUTPUT -o $NETWORK_DEVICE -p UDP \
          -d $NTP_SERVER --dport timeserver \
          -m state --state NEW -j ACCEPT
```

```
  done

# SSH Server
   $IPTABLES -A INPUT -i $NETWORK_DEVICE -p TCP \
          --dport ssh -m state --state NEW -j ACCEPT

# RedHat Network
   $IPTABLES -A OUTPUT -o $NETWORK_DEVICE \
          -p TCP --sport $NON_PRIVAT_PORTS \
          -d $REDHAT_NETWORK_IP_ADDRESS --dport https \
          -m state --state NEW -j ACCEPT

# CVS Server
   $IPTABLES -A OUTPUT -o $NETWORK_DEVICE \
          -p TCP --sport $NON_PRIVAT_PORTS -d\
          $THE_SOURCEFORGE_CVS_SERVER_IP_ADDRESS \
          --dport cvspserver -m state --state NEW -j ACCEPT

# Log all other INPUT traffic
  $IPTABLES -A INPUT -i $NETWORK_DEVICE \
          -m limit --limit 2/s -j LOG --log-level info

# Log all other OUTPUT traffic
   $IPTABLES -A OUTPUT -o $NETWORK_DEVICE \
          -m limit --limit 2/s -j LOG --log-level info
```

7.2.8.4 Install the firewall script

When you have written your firewall script, you must upload it to the server (using scp or sftp, for example). Copy the firewall script (under RedHat) to the following folder and set the rights.

[root@server tmp]# cp egroupware_iptables.sh /etc/sysconfig/

[root@server tmp]# chown root.root /etc/syconfig/egroupware_iptables.sh

[root@server tmp]# chmod 500 /etc/syconfig/egroupware_iptables.sh

Now you can start your IPTABLES script. Check that the rules are loaded and test it.

[root@server tmp]# /etc/syconfig/egroupware_iptables.sh

[root@server tmp]# iptables –L
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT all -- anywhere anywhere

```
ACCEPT     all  --  anywhere            anywhere          state RELATED,ESTABLISHED
DROP       all  --  anywhere            anywhere          state INVALID
DROP       tcp  --  anywhere            anywhere          tcp flags:FIN,SYN,RS T,PSH,ACK,URG/NONE
DROP       tcp  --  anywhere            anywhere          tcp flags:FIN,SYN/FI N,SYN
DROP       tcp  --  anywhere            anywhere          tcp flags:SYN,RST/SY N,RST
<<<--- SNIP ---

--- SNIP --->>>
ACCEPT     tcp  --  anywhere            anywhere          tcp spts:1024:65535 dpt:http state NEW
ACCEPT     tcp  --  anywhere            anywhere          tcp spts:1024:65535 dpt:https state NEW
ACCEPT     tcp  --  anywhere            anywhere          tcp dpt:ssh state NE W
```

When the script is working, you can save the loaded firewall rules with the following command:

```
[root@server tmp]# iptables save
```

7.2.8.5 Firewall logfile analyse

It is easy to activate logging on a firewall when you don't use a tool to analyze the firewall logs. However, It is not possible to receive alarms or warnings from your firewall "in time" when you audit the files by hand.

One tool that automatically analyzes your firewall logs is fwlogwatch [18]. Fwlogwatch is an open source firewall/IDS log analyzer and interactive real-time attack detection and response tool.

7.3 Web Application Security

With web application security software you can secure your web-based applications like eGroupWare from SQL injection, Cross Side Scripting and other attacks. There are several applications on the market for the Apache and IIS web servers. Two tools which are open source are:

ModSecurity [19](for Apache Web server 1.3x and 2.x)
IISShield [20](For Internet Information Server)

ModSecurity is an open source intrusion detection and prevention engine for web applications. It operates embedded into the web server, acting as a powerful umbrella – shielding applications from attacks. ModSecurity supports Apache 1.3x and Apache 2.x.

18 http://fwlogwatch.inside-security.de/
19 http://www.modsecurity.org/
20 http://www.kodeit.org/products/iisshield/default.html

7.3.1 Installing ModSecurity

Unpack the mod_security source archive::

[root@server tmp]# tar xzvf mod_security-x.x.x.tar.gz

Change to the mod_security directory:

[root@server tmp]# cd mod_security-x.x.x/apache2

You can compile the module as an Apache DSO (Dynamic Shared Object) module or statically into the web server. If you compile it statically, you must also recompile Apache. This may yield a slight performance gain, but in general it is not significant. The following example shows only how to compile ModSecurity as a DSO module:

[root@server apache2]# apxs -cia mod_security.c

Under Redhat, add the follow line to your httpd.conf file under the section where the modules are loaded:

[root@server mod_security-1.7.4]# vi /etc/httpd/conf/httpd.conf

Include /etc/httpd/conf.d/mod_security.conf

You must restart your Apache web server to activate ModSecurity:

[root@server mod_security-1.7.4]# apachectl stop
[root@server mod_security-1.7.4]# apachectl start

7.3.2 Basic setup

ModSecurity has some included sample setup files to help you with its configuration. You can also convert Snort rules to use them inside ModSecurity. Sample Snort rules can found on the project server or you can convert them yourself.

.

```
<IfModule mod_security.c>

    # Turn the filtering engine On or Off
    SecFilterEngine On

    # Make sure that URL encoding is valid
    SecFilterCheckURLEncoding On

    # The audit engine works independently and
    # can be turned On of Off on the per-server or
    # on the per-directory basis.  "On" will log everything,
    # "DynamicOrRelevant" will log dynamic requests or violations,
    # and "RelevantOnly" will only log policy violations
    SecAuditEngine RelevantOnly

    # The name of the audit log file
    SecAuditLog logs/audit_log
```

```
    SecFilterDebugLog logs/modsec_debug_log
    SecFilterDebugLevel 0

    # Should mod_security inspect POST payloads
    SecFilterScanPOST On

    # Action to take by default
    SecFilterDefaultAction "deny,log,status:500"

    # Prevent path traversal (..) attacks
    SecFilter "\.\./"

    # Weaker XSS protection but allows common HTML tags
    SecFilter "<[[:space:]]*script"

    # Very crude filters to prevent SQL injection attacks
    SecFilter "delete[[:space:]]+from"
    SecFilter "insert[[:space:]]+into"
    SecFilter "select.+from"

  # Require HTTP_USER_AGENT and HTTP_HOST headers
    SecFilterSelective "HTTP_USER_AGENT|HTTP_HOST" "^$"
</IfModule>
```

Take care! The configuration of ModSecurity depends on the other modules you're using. You must fine-tune your configuration when you receive errors. Only use the filters that are needed for your server. For instance, when you run a Linux-based server, you don't need to test or use the Windows rules.

7.3.3 Testing ModSecurity

You can run a quick test of the functionality of ModSecurity. Change to the test directory in ModSecurity and run some of the example tests:

[root@server tests]# ./run-test.pl yourIpAdress 09-directory-traversal-in-parameters.test 11-xss-attack.test 13-sql-injection.test

Test "09 Directory traversal in parameters": Failed (status = 406)
Test "11 XSS attack": Failed (status = 406)
Test "13 SQL injection": Failed (status = 406)

7.3.4 ModSecurity sample log

This is an example log from the tests above:

```
Request: xxx.xxx.xxx.xxx - - [[21/Feb/2004:20:40:29 +0100]] "GET
/cgi-bin/modsec-test.pl?p=../../tmp/file.txt HTTP/1.0" 406 352
Handler: cgi-script
---------------------------------------
GET /cgi-bin/modsec-test.pl?p=../../tmp/file.txt HTTP/1.0
Host: xxx.xxx.xxx.xxx :80
User-Agent: mod_security regression test utility
Connection: Close
mod_security-message: Access denied with code 406.  Pattern match "\.\./"
at THE_REQUEST.
mod_security-action: 406

HTTP/1.0 406 Not Acceptable
Content-Length: 352
Connection: close
Content-Type: text/html; charset=iso-8859-1
=======================================

Request: xxx.xxx.xxx.xxx - - [[21/Feb/2004:20:40:29 +0100]] "GET
/cgi-bin/modsec-test.pl?p=<script>alert('Bang!')</script> HTTP/1.0" 406
352
Handler: cgi-script
---------------------------------------
GET /cgi-bin/modsec-test.pl?p=<script>alert('Bang!')</script> HTTP/1.0
Host: xxx.xxx.xxx.xxx:80
User-Agent: mod_security regression test utility
Connection: Close
mod_security-message: Access denied with code 406.  Pattern match "<(
|\n)*script" at THE_REQUEST.
mod_security-action: 406

HTTP/1.0 406 Not Acceptable
Content-Length: 352
Connection: close
Content-Type: text/html; charset=iso-8859-1
=======================================
Request: xxx.xxx.xxx.xxx - - [[21/Feb/2004:20:40:29 +0100]] "GET
/cgi-bin/modsec-test.pl?p=DELETE%20FRoM+users HTTP/1.0" 406 352
Handler: cgi-script
---------------------------------------
GET /cgi-bin/modsec-test.pl?p=DELETE%20FRoM+users HTTP/1.0
```

```
Host: xxx.xxx.xxx.xxx
User-Agent: mod_security regression test utility
Connection: Close
mod_security-message: Access denied with code 406.  Pattern match
"delete[[:space:]]+from" at THE_REQUEST.
mod_security-action: 406

HTTP/1.0 406 Not Acceptable
Content-Length: 352
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

7.4 Optimization and securing of the Apache web server

To secure your web server you should disable all unneeded modules. Activate only what you need to run your web applications. Running Apache with fewer modules will also improve its performance.

7.4.1 Recommended modules to run

The following is a short overview of what you need to run Apache 2 with eGroupWare. All other modules can and should be disabled.

Optimization of the Apache web server is **not** for novices! When you disable some modules in your httpd.conf you must also comment out some other options. It is strongly recommended that for each module you are removing, you disable it, stop Apache, and start Apache again, and do this one module at a time! Ensure that you receive no error messages each time.

```
mod_access.so
mod_auth.so
mod_include.so
mod_log_config.so
mod_expires.so
mod_deflate.so
mod_headers.so
mod_unique_id.so
mod_setenvif.so
mod_mime.so
mod_negotiation.so
mod_dir.so
mod_alias.so
```

7.4.2 Other Apache configuration options

You can hide information about your Apache web server for security reasons. There are different possibilities for Apache 1.3 and Apache 2.x.

The **ServerTokens** variable in your httpd.conf file should have the value **OS,** and the **ExtendedStatus** variable should be set to **OFF**. **ServerSignature** should be set to **OFF**, the manual directory **/var/www/manual** to **Deny from all**. When you don't need **cgi-bin** disable it. The **AddHandler** for type-map INCLUDES, send-as comment out with a # symbol at the beginning of the line. Under **/var/www/error** set **Order deny,allow** to **Deny from all**. The **/server-status** and **/server-info** directories should never be publicly readable for security reasons.

7.5 eAccelerator

eAccelerator is a free open source PHP accelerator, optimizer, encoder and dynamic content cache for PHP. It increases performance of PHP scripts by caching them in compiled state, so that the overhead of compiling is almost completely eliminated. Also it uses some optimizations to speed up execution of PHP scripts. eAccelerator typically reduces server load and increases the speed of your PHP code by 1-10 times.

For more information about eAccelerator visit the developer homepage [21].

7.5.1 Requirements

phpize is needed to build the configure script. Check the availability of phpize with search or locate. On Fedora Linux you must install php-devel to compile eAccelerator.

RedHat Enterprise Linux 3 is shipped **without** the phpize package. You must recompile the PHP package and build two devel packages.

7.5.1.1 RedHat Enterprise Linux 3 pre tasks

To build the PHP devel package you need the following packages.

> bzip2-devel curl-devel db4-devel expat-devel freetype-devel gd-devel gdbm-devel gmp-devel pspell-devel httpd-devel libjpeg-devel, libpng-devel pam-devel libstdc++-devel libxml2-devel ncurses-devel openssl-devel zlib-devel pcre-devel imap-devel

The packages **pcre-devel** and **imap-devel** are not offered from RedHat and you must build them yourself. Download the srpm to your server, copy them to /usr/src/redhat/SRPMS, and build the devel packages:

> *[root@server SRPM]#rpmbuild –rebuild pcre-x.x-xx.src.rpm*
>
> *[root@server SRPM]#rpmbuild –rebuild imap-x.x-xx.src.rpm*

Change to the RPM directory and install the needed devel RPMs on your server:

> *[root@server SRPM]#cd /usr/src/redhat/RPM/i386*
>
> *[root@server i386]#rpm –ivh pcre-devel-x.x-xx.i386 imap-devel-xxxxx-x.rpm*

Install the PHP src RPM on your server and change to the SPEC directory

> *[root@server SRPM]#cd /usr/src/redhat/SPEC*

21 http://sourceforge.net/projects/eaccelerator/

You must now edit the php.spec file with vi or vim

After Line 55 add the following lines to the file:

```
%package devel
Group: Development/Libraries
Summary: Files needed for building PHP extensions.

%description devel
The php-devel package contains the files needed for building PHP
extensions.  If you need to compile your own PHP extensions, you will
need to install this package.
```

Change the following line from:

```
$RPM_BUILD_ROOT%{_bindir}/{phptar,pearize,php-config,phpextdist,phpize}
```

To:

```
$RPM_BUILD_ROOT%{_bindir}/{phptar,pearize}
```

Delete this line:

rm -rf $RPM_BUILD_ROOT%{_includedir} |
$RPM_BUILD_ROOT%{_libdir}/php

Add this block after the first %files section:

```
%files devel
%defattr(-,root,root)
%{_bindir}/php-config
%{_bindir}/phpize
%{_bindir}/phpextdist
%{_includedir}/php
%{_libdir}/php
```

Save the file, and build the new package

[root@server SPECS]# rpmbuild –bb php.spec

Install **ONLY** the php-devel package on your server!

7.5.2 Compatibility

This version of the eAccelerator has been successfully tested on PHP 4.1.0-4.3.2 under RedHat Linux 7.0, 7.3, and 8.0; RedHat ES and AS; and Windows with Apache 1.3 and 2.0.

7.5.3 Quick install

Compiling eAccelerator:

export PHP_PREFIX="/usr"
$PHP_PREFIX/bin/phpize
./configure –enable-mmcache=shared –with-php-config=$PHP_PREFIX/bin/php-config
make

You must specify the real prefix where PHP is installed in the "export" command. It may be "/usr" "/usr/local", or something else.

Installing eAccelerator:

make install

Configuring eAccelerator:

eAccelerator can be installed as either a Zend or PHP extension. You will need to edit your php.ini file (usually /etc/php.ini)

To install as a Zend extension:

```
zend_extension=”/usr/lib/php4/eaccelerator.so”
eaccelerator.shm_size=“16“
eaccelerator.cache_dir=“/tmp/eaccelerator“
eaccelerator.enable=“1“
eaccelerator.optimizer=“1“
eaccelerator.check_mtime=“1“
eaccelerator.debug=”0”
eaccelerator.filter=””
eaccelerator.shm_max=”0”
eaccelerator _ttl=”0”
eaccelerator.shm_prune_period=”0”
eaccelerator.shm_only=”0”
eaccelerator.compress=”1”
```

If you use a thread-safe build of PHP you must use “zend_extensions_ts” instead of “zend_extension”

To install as a PHP extension:

```
extension=”eaccelerator.so”
eaccelerator.shm_size=“16“
eaccelerator.cache_dir=“/tmp/eaccelerator“
eaccelerator.enable=“1“
eaccelerator.optimizer=“1“
eaccelerator.check_mtime=“1“
eaccelerator.debug=”0”
eaccelerator.filter=””
eaccelerator.shm_max=”0”
eaccelerator _ttl=”0”
eaccelerator.shm_prune_period=”0”
eaccelerator.shm_only=”0”
eaccelerator.compress=”1”
eaccelerator.content
```

Creating the cache directory:

mkdir /tmp(mmcache

chmod 0777 /tmp/eaccelerator

7.5.4 Web interface

eAccelerator can be managed through the web interface script eaccelerator.php, so you'll need to put this file on your web site. For security reasons it is recommended to restrict the usage of this script to your local IP.

Since version 2.3.18 the admin interface may be protected by a password. To generate a password run the eaccelerator_password.php file from a command line and follow the instructions.

Create the eAccelerator password:

*[root@server eaccelerator***]# php –q eaccelerator_password.php*

Changing password for eAccelerator Web Interface (eaccelerato.php)

Enter admin name: cacheadminname

New admin password: yourpassword

Retype new admin password: yourpassword

Add the following lines into your php.ini and restart HTTPD

eaccelerato.admin.name="cacheadminname"

eaccelerato.admin.password="$1$0ScD9gkb$nOEmFerNMvQ576hELeLrG0"

7.6 Securing the PHP installation

Secure your web server directories so they are only visible by your web server user.

```
;;;;;;;;;;;;;;;;;;;
; Language Options ;
;;;;;;;;;;;;;;;;;;;

; open_basedir, if set, limits all file operations
; to the defined directory
; and below.  This directive makes most sense if used in a per-directory
; or per-virtualhost web server configuration file.
open_basedir =
var/www/html:/var/www/files:/tmp:/usr/share/pear:/usr/bin/crontab

; Decides whether PHP may expose the fact that it is installed on the
server e.g. by adding its signature to the Web server header).
; It is no security threat in any way, but it makes it possible to
; determine whether you use PHP on your server or not.
expose_php = Off

;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;;
max_execution_time = 30 ; Maximum execution time of each script,
inseconds
memory_limit = 24M ; Maximum amount of memory a script may consume (8MB)

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Error handling and logging ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

; Print out errors (as a part of the output).  For production web sites,
; you're strongly encouraged to turn this feature off, and use error
; logging instead (see below).  Keeping display_errors enabled on a
; production web site may reveal security information to end users, such
; as file paths on your Web server, your database schema or other
; information.
display_errors = Off

; Even when display_errors is on, errors that occur during PHP's startup
; sequence are not displayed.  It's strongly recommended to keep
; display_startup_errors off, except for when debugging.
display_startup_errors = Off
```

```
; Log errors into a log file (server-specific log, stderr,
; or erro_ log (below)) As stated above, you're strongly advised to use
error logging in place ; of error displaying on production web sites.
log_errors = On

; Store the last error/warning message in $php_errormsg (boolean).
track_errors = Off

; Log errors to syslog (Event Log on NT, not valid in Windows 95).
error_log = syslog

;;;;;;;;;;;;;;;;;;
; Data Handling ;
;;;;;;;;;;;;;;;;;;

register_globals = OFF
```

It is more secure to set the paths for session.save_path and upload_tmp_dir in your php.ini file and include them in the open basedir restrictions.

7.7 Creating a web server certificate

To protect your privacy, you can use a server certificate when you connect to your eGroupWare installation. With a certificate you can connect to your web server with an encrypted connection (using **https** instead of **http**). Without an https connection, other people can sniff your password or other personal information.

You have a few possibilities when creating a web server certificate:

1.) Create your own certificate authority and self-sign your server certificate.

(Trust is low)

2.) Use a non-Profit Certificate Authority.

CAcert [22]

(Trust is high)

3.) Use a commercial Certificate Authority.

Thawte [23]

Verisign 24

(Trust is high)

If you want to use a commercial Certificate Authority, please go directly to create your server key and

22 https://www.cacert.org

23 http://www.thawte.com

24 http://www.verisign.com

signing request

7.7.1 Joining CA Cert

The first step to receiving a server certificate is joining CAcert.

Open your browser and go to the following URL: https://www.cacert.org.
Follow the link on the left side to join CAcert.
Proceed with enrollment.
Fill out all the necessary information to receive your personal account at CAcert.
After you have submitted your password, you will receive more instructions via Email.

7.7.2 Creating your certificate signing request

On your server installation you must create a server key and a certificate signing request.

7.7.2.1 Changing the openssl.cnf file

You will need to make changes in the openssl.cnf file only if you want use the certificate from the non-profit Certificate Authority (CAcert). Under Debian Linux you will find the file under /usr/lib/ssl/ and for Red Hat the path is /usr/share/ssl/

Please check that your openssl.cnf looks like the following snippet. The important lines here are the lines which are commented out or the change in the stateOrProvinceName value.

[root@server ssl]# vi openssl.cnf

```
# For the CA policy
[ policy_match ]
countryName                     = match
stateOrProvinceName             = optional
organizationName                = match
organizationalUnitName          = optional
commonName                      = supplied
emailAddress                    = optional

[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = GB
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName              = State or Province Name (full name)
localityName                     = Locality Name (eg, city)
0.organizationName               = Organization Name (eg, company)
organizationalUnitName           = Organizational Unit Name (eg, section)
```

7.7.2.2 Creating your server key and signing request

To get a certificate, you must create a server key and a server certificate signing request.

1.) Create a server key. The server key is stored under Debian in the folder /etc/ssl/certs/ and under Red Hat in /etc/httpd/conf/ssl.csr/

The following command creates a server key which is password protected. If you have no console access to your server, **DON'T** create a password protected key. Your server will wait for a password on boot and will not start until you provide the password. If you have console access, use the password protected key! It is more secure.

[root@server ssl]# /usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter PEM pass phrase:

To create a key which is **not password protected:**

[root@server ssl]# /usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key

Change the access rights for your key:

[root@server ssl]# chmod go-rwx /etc/httpd/conf/ssl.key/server.key

2.) Now you must create your certificate signing request. Please remember to change the paths to your server paths for the keys.

[root@server ssl]# /usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:

The system asks you for the password, which you gave when you created the key. If you created a key without password protection, a password isn't needed.

You are about to be asked to enter information that will be incorporated
into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:DE
State or Province Name (full name) []:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:egroupware.org
Organizational Unit Name (eg, section) []:
Common Name (your name or server's hostname) []:egroupware.org
Email Address []:yourname@yourdomain.org
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

In your folder, you will find a new file named server.csr. This file has to be sent to your certificate authority.

7.7.2.3 Sending the signing request to your CA

The certificate signing request has to be sent to the certificate authority. Here we send it to CAcert.

1. Open your Browser and go to the following URL. https://www.cacert.org.
2. Follow the link Server Certificate -> Login.
3. Add a new domain.
4. Confirm the email that is sent to you.
5. Follow the link Certificates -> Requests.
6. Copy the whole content of your server.csr file into the text field.
7. Agree with the process.

7.7.2.4 Installing the server certificate.

After submitting your CSR, you will receive an email from your CA with your signed certificate. The whole body of the Email has to be copied to a file name server.crt on your server.

After saving the file, you need to restart your web server.

7.8 The web server

Secure your web server directories, so they are only visible by your web server user.

[root@server html]# chown -R root:webserveruser egroupware

[root@server html]# find egroupware -type d -exec chmod 550 {} \;

[root@server html]# find egroupware -type f -exec chmod 440 {} \;

We strongly recommend securing your Apache directory. Please add the following lines to your httpd.conf:

```
<Directory /var/www/html/egroupware>
                    <Files ~ "\.(inc.php|tpl)$">
                              Order allow,deny
                              Deny from all
                    </Files>
</Directory>
```

7.9 Secure the SQL server

MySQL

Be sure that your database runs and automatically starts when your server boot

When you set up your MySQL server for the first time, don't forget to set the MySQL server root password. The password in a standard installation is **EMPTY**. When you don't set up a root password for your MySQL server, every user with shell access can login to your MySQL server without a password!.

To set a MySQL password use the following command:

[root@server html]# mysqladmin –u root password 'new-password'

The MySQL server includes a test database. This database is not needed in production environments. Drop this database.

[root@server html]# mysql –u root –p
Enter Password:
mysql>drop database test;
Query OK, 0 rows affected (0,03 sec)

For the MySQL database add the following parameter to make sure that your MySQL server can only be used via localhost. Change your /etc/my.cnf and add the following line:

```
[mysqld]
bind-address=127.0.0.1
```

7.10 Backup and restore your database!

Groupware is mission critical software in your IT environment. If you lose your groupware software, along with all of the information stored in it (calendar information, contacts, knowledge base entries, trouble tickets, etc.) it can be a disaster for your company or yourself.

The database, the directories used by eGroupWare outside the web server's root and the header.inc.php files are all needed to restore an eGroupWare installation from scratch. There are several professional backup tools on the market to make a backup from your eGroupWare installation. If you do not have access to those tools, however, some simple ways to perform backups will be shown.

You can also use the backup application shipped with eGroupWare itself. This will work for a single installation of eGroupWare on a server – but what do you do if there are several installations you need to back up? What if your web server is down? For these reasons, you should also understand how to backup from the command line.

7.10.1 Decide your backup solution

Your backup strategy depends on the time you have to setup a new groupware server: how long your users can "live" without the groupware software and the information it provides.

Requirements	YES		NO	
Your users can live without the groupware software for more the 6 hours?	✔	☐	✔	☐
Your database and file sizes will be less than a few hundred megabytes?	✔	☐	✔	☐
You have a server on which you can temporarily install the groupware software while the main server is restored?	✔	☐	✔	☐
You can set up a complete server, including operating system, in-house/alone?	✔	☐	✔	☐

If you answer one or more questions with **NO**, you should use a professional backup solution and not these simple scripts which we provide here to backup your server. There are many commercial solutions available but also open source backup solutions with which you can backup a complete server (such as bacula [25]).

25 http://www.bacula.org/

7.10.2 Backup the MySQL database

7.10.2.1 Manualy backup the MySQL database

To manually make a backup of your database, you can use the following command:.

[root@server html]# mysqldump –u yourmysqladmin -p - -opt database > /directory/database.sql

When you use mysqldump without the –opt flag, the complete backup will first be written to memory and then to the file! This can be a problem if you are backing up large databases.

7.10.2.2 Backup your MySQL with a daily cronjob

Copy this script to your /etc/cron.daily directory (or wherever your daily cron scripts should be placed for your distribution) and make it executable.

```
#!/bin/sh
# The name from the database which you want to backup
db_name="yourdbname"

# The username to connect the database
dbusername="dbuser"

# The password to connect the database
dbuserpassword="dbpassword"

# The directorty outside the webserver root we must backup.
# Please provide the complete path to this directory
files_directory="/var/www/files"

# The path to the egroupware root, as example /var/www/html/egroupware
webserver_root="/var/www/html/egroupware"

# In which directory you want to store the backup
backup_directory="/your/backup/dir"

# Path to the backup log
log=/var/log/db_backup

# The name under which we store the backup
backup=$backup_directory/$db_name-`date +%Y%m%d%H%M`.sql
echo `date`": starting backup of DB $db_name to $backup" >>$log

# create the DB backup
```

```
mysqldump --user=$dbusername --password=$dbuserpassword --opt $db_name
2>>$log > $backup

# zip the backup file
bzip2 $backup 2>&1 >> $log
echo `date`": backup of DB $db_name finished" >>$log

# bzip the directory outside the webserver root
tar cjvf $backup_directory/files-`date +%Y%m%d%H%M`.bz2 $files_directory

# Copy the header.inc.php file to the backup directory
cp $webserver_root/header.inc.php $backup_directory/header.inc.php-`date
+%Y%m%d%H%M`

# Delete backups which are older than X days
cd $backup_directory

find . -name "$db_name-*.sql.bz2" -mtime +14 | \
xargs --no-run-if-empty rm –f

find . -name 'files-*.bz2' -mtime +14 | xargs --no-run-if-empty rm -f
find . -name 'header.inc.php-*' -mtime +14 | \
xargs --no-run-if-empty rm -f
```

7.10.2.3 Restore the MySQL database

To restore your database, you must create the database and restore the data from your backup file:

[root@server html]# mysqladmin –u yourmysqladmin –p create yourdatabase
[root@server html]# mysql –u yourmysqladmin –p < /directory/database.sql

7.10.3 Backup the PostgreSQL database

7.10.3.1 Manualy backup the PostgreSQL database

To manually make a backup from your database, you can run the following command:

[root@server html]# su – postgres
-bash-2.05b$ pg_dump –C –d –F t –b database -f /directory/database.tar

7.10.3.2 Create a cron job for the PostgreSQL srcipt

You must create a cron job for the user postgres to start the daily backup shell script.

[root@server html]# crontab –u postgres –e

Add the following line to the file and save it. This will run your backup script daily at 10 pm.

0 22 * * * /bin/bash /path/to/the/backup/script

PostgreSQL backlup shell script

```
#!/bin/bash
# The name from the database which you want to backup
db_name="yourdbname"

# The directorty outside the webserver root we must backup.
# Please provide the complete path to this directory
files_directory="/var/www/files"

# The path to the egroupware root, as example /var/www/html/egroupware
webserver_root="/var/www/html/egroupware"

# In which directory you want to store the backup
backup_directory="/your/backup/dir"

# Path to the backup log
log=”/var/log/db_backup”

# The name under which we store the backup
backup=$backup_directory/$db_name-`date +%Y%m%d%H%M`.tar
echo `date`": starting backup of DB $db_name to $backup" >>$log

# Clean and analyse a PostgreSQL database
/usr/bin/vacuumdb --d $db_name --analyze
```

```
# create the DB backup
pg_dump --create --inserts --format=t --blobs $db_name --file $backup
2>>$log

# bzip the directory outside the webserver root
tar cjvf $backup_directory/files-`date +%Y%m%d%H%M`.bz2 $files_directory

# Copy the header.inc.php file to the backup directory
cp $webserver_root/header.inc.php $backup_directory/header.inc.php-`date
+%Y%m%d%H%M`

# Delete backups which are older than X days
cd $backup_directory

find . -name "$db_name-*.tar" -mtime +14 | xargs --no-run-if-empty rm -f
find . -name 'files-*.bz2' -mtime +14 | xargs --no-run-if-empty rm -f
find . -name 'header.inc.php-*' -mtime +14 | \
xargs --no-run-if-empty rm -f
```

7.10.3.3 Restore the PostgreSQL database

To restore your PostgreSQL database you can run the following command as user postgres.

[root@server html]# su – postgres
-bash-2.05b$ pg_restore -f /directory/database.tar –F t –d database

8 Setup eGroupWare

8.1 Creating your database

eGroupWare can automatically create the database for you. At the moment this works with MySQL, MSSQL and PostgreSQL databases! If you want eGroupWare to create your databases automatically, proceed to section 8.5.1.

8.1.1 Create the MySQL database

Create your database and a user which can connect to it.

Create the database:

[root@server html]# mysqladmin –u yourmysqladmin –p create yourdatabase
Enter password:

Create the user and give him DB rights:

[root@server html]# mysql –u yourmysqladmin –p
Enter password:
mysql> grant all on egroupware. to egroupwaredbuser@localhost*
identified by "password"

8.1.2 Create the PostgreSQL database

Validate that a connection to your database is possible.

From your ROOT account change to the postgres account:

[root@server html]# su - postgres

Edit the file postgresql.conf:

-bash-2.05b$ cd data
-bash-2.05b$ vi postgresql.conf

Your file should look like the example here:

```
#Connection Parameter
tcpip_socket = true
#ssl = false
#max_connections = 32
port = 5432
```

Edit the file pg_hba.conf so that it looks like our example:

```
# TYPE DATABASE USER IP_ADDRESS MASK AUTH_TYPE AUTH_ARGUMENT
local egroupware trust
host egroupwaredbname all 127.0.0.1 255.255.255.255 md5
```

The USER value appears in PostgreSQL 7.3.X and above.

Restart you PostgreSQL server and test the connectivity:

[root@server html]# /etc/init.d/postgresql restart

[root@server html]# su - postgres

bash-2.05b$ psql -h localhost template1

Close the database connectivity:

template1=# \q

Set up your PostgreSQL database.

Create a user which has rights to access the eGroupWare DB:

bash-2.05b$ createuser yourdbusername –P

Answer the next questions with yes:

bash-2.0.5b$ Shall the new user be allowed to create databases? (y/n) Y

bash-2.0.5b$ Shall the new user be allowed to create more new users? (y/n) N

Create the new eGroupWare database:

bash-2.05b$ createdb -U yourdbusername yourdatabasename

8.2 How to start the setup?

Point your Browser to your server URL to open the setup menu:

https://www.yourserver.com/egroupware/setup

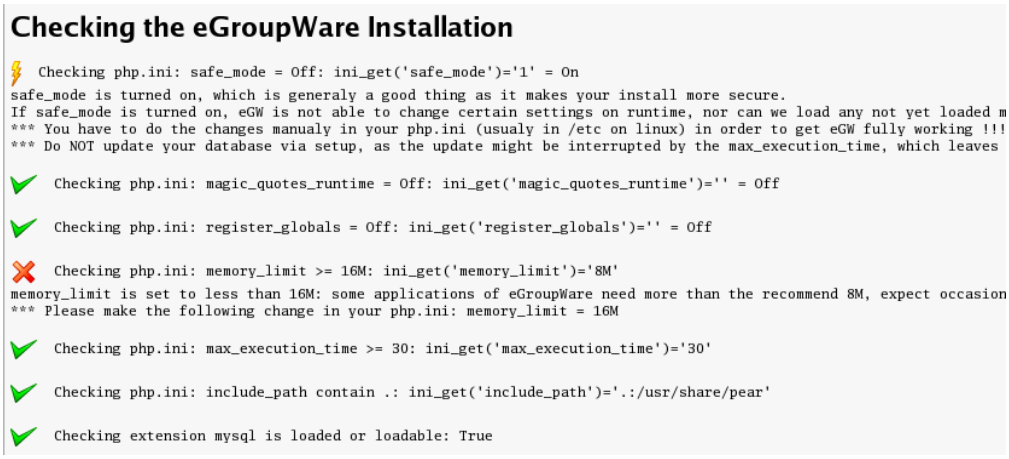
You will automatically be redirected to a check of the eGroupWare installation, which is our next step.

8.3 Checking the eGroupWare installation

If no header.inc.php file is found, eGroupWare runs a check verifying some configuration parameters in your php.ini file and in your local file system. The check shows you errors and warnings that will help you solve any configuration problems.

Errors are shown with a red cross and must be solved by you!

Warnings may be ignored, but should probably be fixed. For example, you may see a warning from the check for safe_mode. If you know how to configure the safe mode restrictions it will be no problem for you, but for new users it is often better to disable this function.



8.4 Creating your header.inc.php

Most parts in the setup for your header.inc.php are self-explanatory. This menu is available in other languages then English, but it may not be translated to your own language yet.

At the moment eGW supports MySQL, PostgreSQL and MSSQL. MaxDB support for eGroupware is on the way

With the Domain select box, you can setup more than one eGroupWare installation. For example, you could have an installation for your employees to work with and a separate one as a training environment.

If you set up your database manually, like in step 6.1, you have given the database a name, user, and password. If you want the eGroupWare setup program to create the database automatically you must first provide the values here.

When you have the possibility, limit the access to eGroupWare setup page!. It protects your installation as example again brute force attacks. You can protect the access as example to a IP address (183.12.34.87), to a subnet (192.168.0) or to a hostname (myhostname.mynet.org)

The following fields describe which database you want to use for eGroupWare and the database user which can connect to the eGroupWare database. Don't use your database administrator to connect to the database. Create a separate user!

DH Host	If your DB runs on the same machine as your eGroupWare installation, it will be localhost. You can also use a separate server to run your DB on.
DB Name	The name of the database that you want to create on your DB Server.
DB User	The user which eGroupWare uses to connect to the database.
DB Password	This password of the DB user.
DB Type	Your DB type.

Download the created header.inc.php file to your local machine, then copy it to your eGroupWare installation's root directory and change the access rights so that only the web server has read access to this file.

[user@server tmp]$ scp header.inc.php youregwserver:/tmp
[user@server tmp]$ ssh youregwserver
[user@youregwserver user]$ su –
Password:
[root@server root]# mv /tmp/header.inc.php /var/www/html/egroupware; chmod 400 /var/www/html/egroupware/header.in.php;
chown apache /var/www/html/egroupware/header.in.php

Continue in your browser to go to the next step.

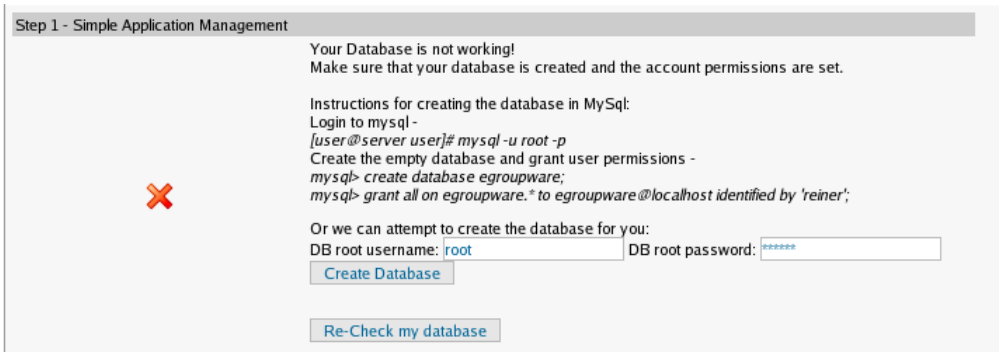
8.5 Setup / Config Admin

After you have finished creating the header.inc.php file and have continued to the next page, you will see two login prompts. Log in to the **Setup/Config Admin Login** with the username and password you provided in the previous step (8.4)

8.5.1 Step 1 – Simple Application Management - Create your database

Here you have two possibilities: If you want to create your database in this step automatically, then go to **create your database** now. If you have created your database manually, then go to **create your tables.**

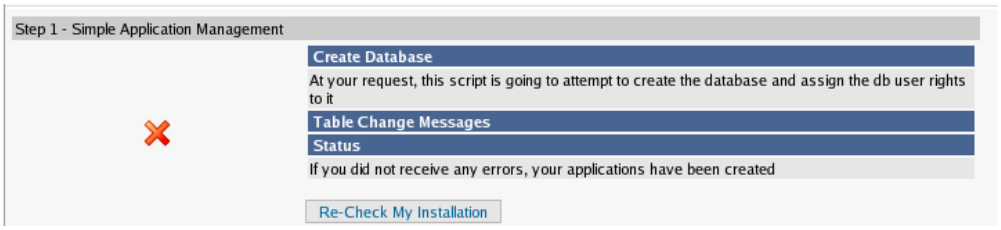
Create your database:



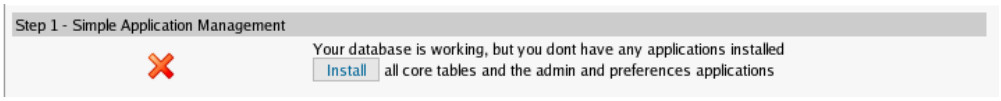
Fill out the following form to create your database automatically:

DB root username	rootusername
DB Password	yourDBrootpassword

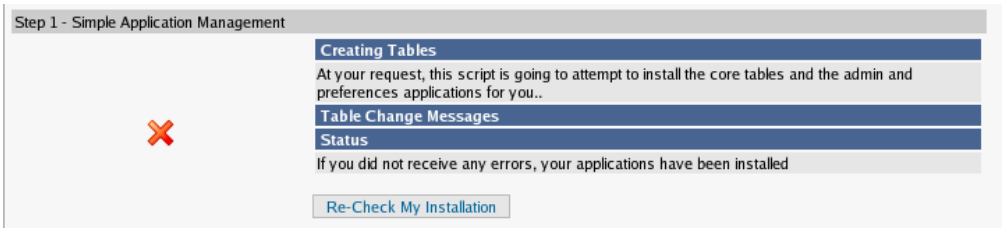
Click "Create Database."



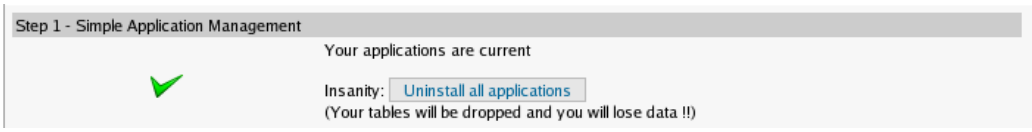
Click Re-Check My Installation:



If you see **no** errors, you can install the tables. Click Install:



Now, take a look at the status. If you see no errors here, continue with Re-Check My Installation:



8.5.2 Step 2 – Configuration

Most parts in this step are self-explanatory. Only some oft-misunderstood information is provided here.

8.5.2.1 Creating the files folder

You have to create the **files** directory manually at the shell prompt. eGroupWare will store attachments from Infolog, files saved in the Filemanager module, and some other files in this directory.

This directory must be **outside** of your web server root! If you don't know where your web server root is, take a look at your httpd.conf file or run the following command under Linux:

[root@server www]$ cat /etc/httpd/conf/httpd.conf | grep ^DocumentRoot
DocumentRoot "/var/www/html"

Create the files directory:

[root@server www]$ mkdir /var/www/files

You have to give the web server the rights to read and write to these directories:

[root@server www]$ chown –R apache.apache /var/www/files
[root@server www]$ chmod –R 0700 /var/www/files

8.5.2.2 Editing the current configuration

Path information

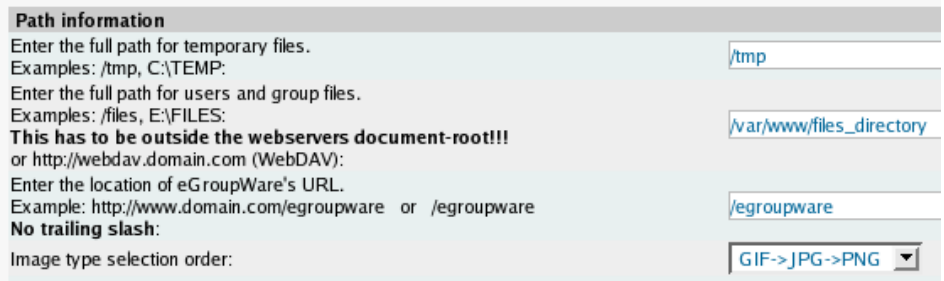
Enter the necessary values for your Path information

The tmp directory is needed to store sessions and other information from your eGroupWare installation. When your run your eGroupWare installation in a change root (chroot) environment or with open_basedir restrictions in your php.ini, the path for the tmp directory must adhere to these restrictions too.

The full path for user and group files **must** be outside the web server root for security reasons. It is not possible to have this directory inside your web server root!

Enter the location of the eGW URL. If you want to use HTTPS and HTTP connections, use /egroupware (if you want to **force** HTTPS then use https://yourdomain/egroupware).

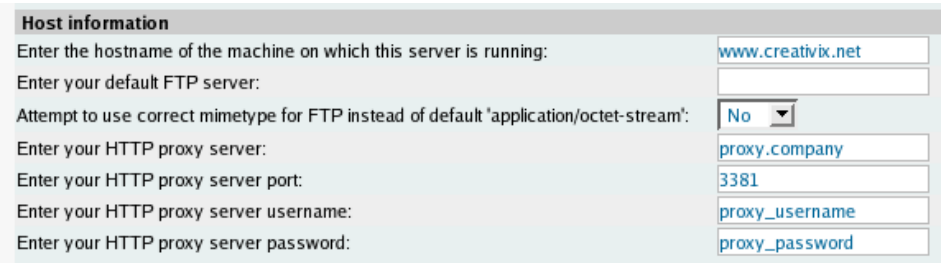
Please don't change the image type selection order from its default (which may be different than the example shown below). It can break the design of the UI.



Host information

Enter the hostname of your server. It must be a valid DNS name or an IP address under which the installation will be run.

When your eGroupWare installation is located behind a Proxy Server (like SQUID) and you want to use applications that connect to remote Internet sites, such as headlines or stocks, you must set up the proxy values.



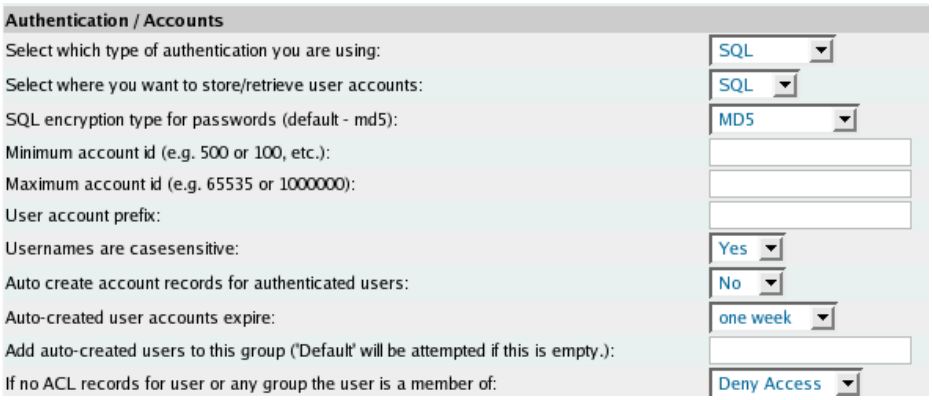
Authentication/Accounts

There are several authentication types available: SQL, SQL/SSL, LDAP, Mail, HTTP, NIS and PAM. Select which type you want to use to authenticate your eGroupWare users.

Select the encryption type for user passwords. The user passwords will be stored encrypted in your database.

When you want to use one LDAP tree for different eGroupWare installations for authentication, you can use the account prefix.

Use case-sensitive usernames for better security.

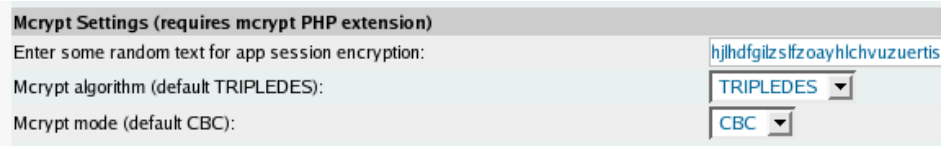


If using LDAP

If you don't want to use LDAP, it is not necessary to fill in these fields. If you want to use LDAP, please take a look at **phpgwapi/doc/ldap/README**.

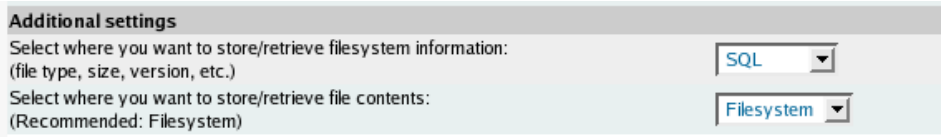
Mcrypt settings (requires the mcyrpt PHP extension)

Not all distributions have a working mcrypt compiled into them by default, so you will need to check this. Also, you may need to try several algorithms and modes to see which works best with eGroupWare given your particular PHP and mcrypt version.



Additional settings

The standard values here are OK.



When you are finished, save your configuration.

8.5.3 Step 3 – Set Up Your User Accounts

Here you create your eGroupWare admin account. Don't use an admin username like admin, administrator, root, etc. For your admin password, use letters, numbers and special characters. Don't create Demo accounts in production environments!

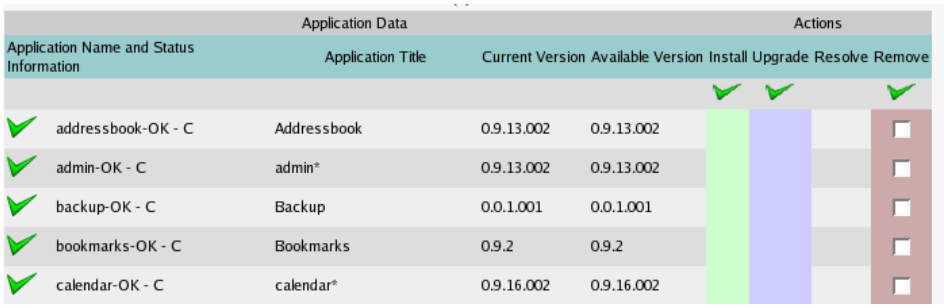
8.5.4 Step 4 – Manage Languages

The standard languages that will be installed are English and the language which you have activated as the default language in your browser (if it is different than English). It is possible to install more languages.

You can convert your system-charset automatically, i.e. from ISO-8859-1 to UTF-8.

8.5.5 Step 5 – Manage Application

In the standard installation, all applications are installed. To uninstall any application, check the Remove checkbox for that application and click Save. If you receive an error message about dependencies, you may have to install another application. For example, felamimail requires emailadmin to run.

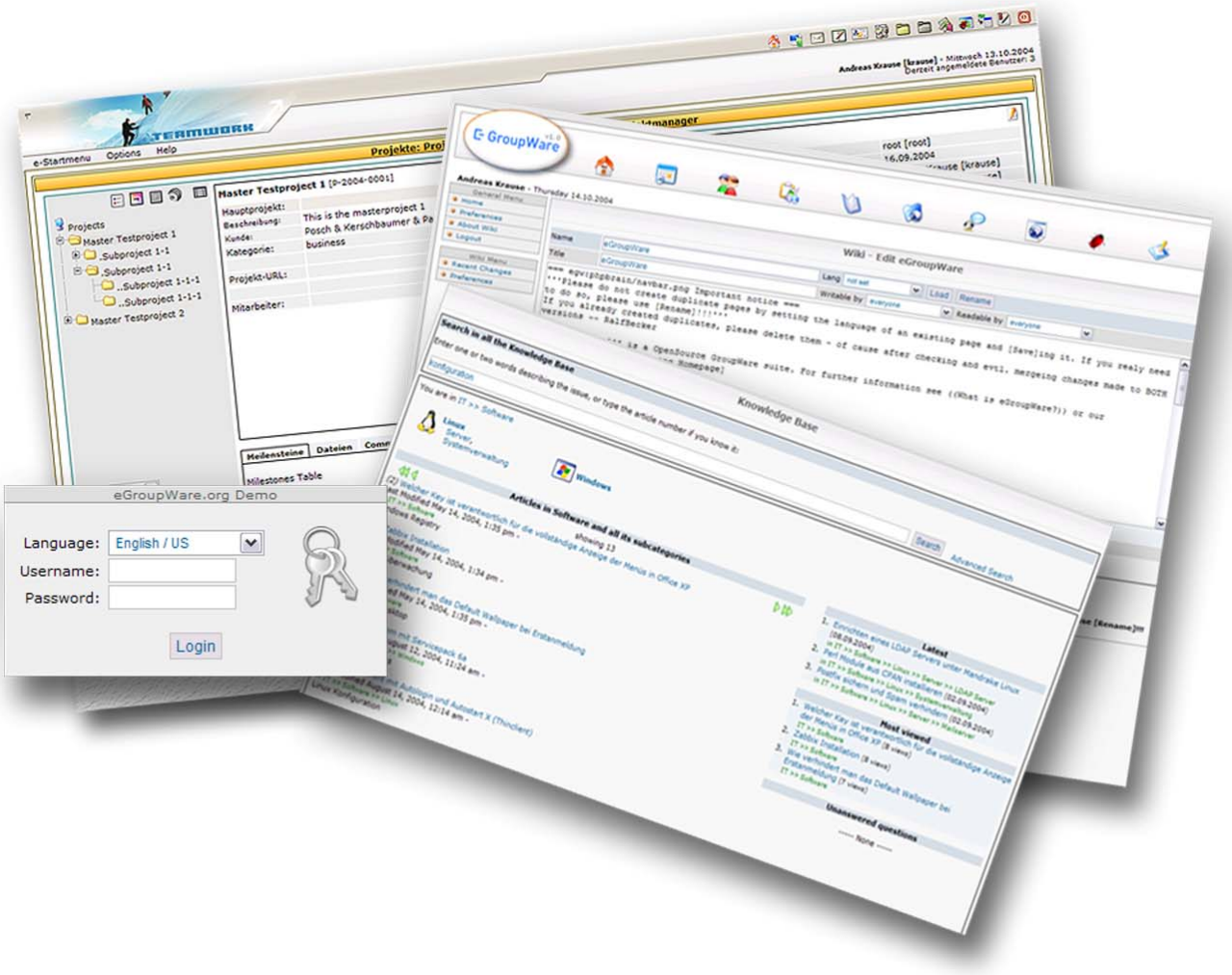


Application Data				Actions			
Application Name and Status Information	Application Title	Current Version	Available Version	Install	Upgrade	Resolve	Remove
addressbook-OK - C	Addressbook	0.9.13.002	0.9.13.002				☐
admin-OK - C	admin*	0.9.13.002	0.9.13.002				☐
backup-OK - C	Backup	0.0.1.001	0.0.1.001				☐
bookmarks-OK - C	Bookmarks	0.9.2	0.9.2				☐
calendar-OK - C	calendar*	0.9.16.002	0.9.16.002				☐

9 Log In to eGroupWare

Once you have finished your setup of eGroupWare, you can log in. Go to http://yourdomain/egroupware (or https://yourdomain/egroupware, if appropriate).

The first step as admin should be to go to the admin interface and set up your site configuration, users and groups, email settings and other necessary information.



10 Troubleshooting

10.1 Forgot the admin password

I forgot my admin password and can't log in with my admin user to eGroupWare!

Go to http://yourserver.com/egroupware/setup
Log in to Setup/Config Admin Login
Set up a new admin account.

10.2 Admin user or other user is blocked

I can't log in anymore to my eGroupWare installation. I receive: Blocked, to many attempts. What can I do?

Using a standard configuration, you must wait 30 minutes to be able to log in again. This is a security feature -- don't disable it!

10.3 Database error: lock(Array, write) failed

Database error: lock(Array, write) failed
MySQL Error 1044 (Access denied for user '@localhost' to database 'groupware')
Function: db::halt / db::lock / config::save_repository / sessions::sessions_ / session_sessions / createobject / include / include
session halted

Check the permissions of your database. Your user does not have all necessary rights.

10.4 Checking file permissions

This error is occurring when I run the Check Installation script:

Checking file-permissions of ./phpgwapi/images for not worldwritable: hri/users drwx---rwx
./phpgwapi/images is world writeable!!!

Change the rights in the directory phpgwapi/images so it is not world-writeable:

chmod 700 images

10.5 Cannot get past the Check Install page (#1)

There are no warnings or errors.....I install the header.inc.php file with all of the correct values, etc., but I keep ending up back at that bloody check_install.php page...

Check that the web server has the rights to read the header.inc.php file and that the file is in your eGroupWare root.

10.6 Cannot get past the Check Install page (#2)

We installed eGroupWare on a Linux box that also has a proxy server installed.

Clients are using Microsoft Internet Explorer that has a reference to the proxy server, although the proxy server should be bypassed (options->connection->proxy->advanced settings).

We are not able to upload attachments greater than 1 Mb. Everything in php.ini and httpd.conf was applied, but we are still not able to upload >1 MB

Proxy servers often must be configured to allow a stream through that is greater than a certain default size. For instance, in Squid, you need to change the "request_body_max_size" from its default of 1MB.

eg: request_body_max_size 20 MB

10.7 Windows: fudforum/3814******9): Permission denied

Warning: mkdir(D:\Websites\yourwebsite\egroupware\fudforum/3814******9): Permission denied in D:\Websites \egroupware\fudforum\setup\default_records.inc.php on line 114

ERROR: Failed to create D:\Websites\yourwebsite\egroupware\fudforum/38145******, please create this directory manually and chmod it 777SiteMgr demo site installed

Simply went in and created the directory 3814****** under D:\Websites\yourwebsite\egroupware\fudforum directory and gave it read and write permissions. Please Note: the "3814******" number will be the CRC32 of your domain, so it will be different with each machine."

**This taken from the D:\websites\yourwebsite\fudforum\setup\readme file – "The \fudforum\setup\index.php file will need to create several files inside the web browseable fudforum\ directory. This will require you to grant write permissions to the web-server to several files and directories (installer will complain about them, if they are not writable). The simplest solution is to temporary give the fudforum/ directory full access permissions and then restore to normal permissions (read and write) once the installation process is complete. If you wish to save a few megabytes of space, once the forum is installedyou can remove the base/ directory, it is no longer needed."

10.8 Sitemgr: mkdir(./sitemgr-link): Permission denied

Warning: mkdir(./sitemgr-link): Permission denied in D:\Websites\calvarycentral\egrouptest\egroupware\sitemgr\setup\default_records.inc.php on line 165

Can't mkdir(./sitemgr-link) !!!sitemgr/sitemgr-link copied to eGroupWare dir and sitemgr-link NOT installed, you need

to copy it from egroupware/sitemgr/sitemgr-link to egroupware/sitemgr-link and install

- Copy the sitemgr-link folder from \egroupware\sitemgr\ that was created by eGroupWare and placed it in the root folder of D:\Websites\yourwebsite\egroupware. This enables you to install it from the "Manage Applications" link on the /egroupware/setup/index.php page.

10.9 Error 1250 (Client does not support authentication protocol requested by server

If you're using MySQL version 4.1 or higher and you've been getting database errors trying to set up eGW, this will probably fix the problem:

MySQL 4.1 by default uses a new password authentication protocol that is incompatible with the current release of eGroupWare.

If you attempt to let eGroupWare create the database for you using the MySQL root user, it fails with the following error:
Error 1250 (Client does not support authentication protocol requested by server ...

- To fix this, you must first edit your MySQL configuration by either starting with the --old-passwords command line option or by adding the following to your my.ini file:

  #Use old password encryption method (needed for 4.0 and older clients).
  old-passwords

  Now update the MySQL user(s) passwords with the following command:

  mysql> SET PASSWORD FOR -> 'some_user'@'some_host' = OLD_PASSWORD('mypass');

10.10 Create a admin account but can't login

I create in setup a admin account but when I want login, I receive wrong username or password. With the created demo account, login is possible.

- Some username are not allowed as eGroupWare usernames. They are blocked when you use it as usernames.

  root, bin, daemon, adm, lp, sync, shutdown, halt, ldap, mail, news, uucp, operator, games, gopher, nobody, xfs, pgsql, mysql, postgres, oracle, ftp, gdm, named, alias, web, sweep, cvs, qmaild, qmaill, qmaillog, qmailp, qmailq, qmailr, qmails, rpc, rpcuser, amanda, apache, pvm, squid, ident, nscd, mailnull, cyrus, backup

10.11 Loop when creating database

I running in a endless loop when create the database in setup

Please test it with another browser. Some versions of Internet Explorer cause problems.

10.12 Check with what modules php is compiled

I have a problem during my attempt to install egroupware in my computer.
The problems message is: Checking extension mssql is loaded or loadable: False

I changed the php.ini and i add the line:extension=php_mssql.dll
But then when i tried to check installation the next window appeared:
Unknown():Unable to load dynamic library'./php_mssql.dll'-The specified module could not be found

This problem occurred due to PHP not being able to find a file named php_mssql.dll in its installed directory (default is C:\php). Following these steps:
1. Start->Run->cmd. At the command prompt, change to your PHP directory (i.e. C:\PHP, using the appropriate path for your system).
2. type php -v , hit Enter and remember your PHP version.
3. Go to http://www.php.net/releases.php and download the zip package (Windows binary) of your PHP version.
4. Extract the zip package to a folder. Change to that folder, then to the extensions subfolder. Copy the php_mssql.dll file to your PHP directory.

10.13 mbstring error at install

During the check install script, I receive an error about missing mbstring, or other similar errors..

Use the following command from the command line to find out what is compiled into PHP in your distribution:

php –m

10.14 PHP include path error message

I get the following error message:

Checking php.ini: include_path contain
.: ini_get('include_path')='./:/usr/local/lib/php'
include_path need to contain "." - the current directory

include_path = .:./:/usr/local/lib/php

11 Software Map

AIDE, Advanced Intrusion Detection System

Platform	Linux / BSD / *nix
License	**GPL**
Homepage	sourceforge.net/projects/aide
Download	
RPM	Take a look at your distribution
DEB	Debian Project
tar.gz	AIDE Project file server

Apache Web server project

Platform	Linux / BSD / Win / other
License	Apache Software License
Homepage	httpd.apache.org
Download	
RPM	Take a look at your distribution
DEB	Debian Project
tar.gz	Apache Project file server
Win	Apache Project file server

Bacula – The Network Backup Solution

Platform	Linux / BSD / Win / other
License	GPL / LGPL
Homepage	www.bacula.org
Download	
RPM	sourceforge.net bacula project
DEB	sourceforge.net bacula project
tar.gz	sourceforge.net bacula project
Win	sourceforge.net bacula project

chkrootkit project

Platform	Linux / BSD
License	**BSD-Like**
Homepage	www.chkrootkit.org
Download	
RPM	creativix chkrootkit page
tar.gz	chkrootkit project

eAccelerator

Platform	Linux / BSD / Win / other
License	**GPL**
Homepage	sourceforge.net/projects/eaccalerator
Download	
tar.gz	eAccelerator project
tar.bz2	eAccelerator project
zip	eAccelerator project

eGroupWare project

Platform	Linux / BSD / WIN / other
License	**GPL**
Homepage	www.egroupware.org
Download	
RPM	sourceforge.net eGroupWare project
tar.gz	sourceforge.net eGroupWare project
tar.bz2	sourceforge.net eGroupWare project
zip	sourceforge.net eGroupWare project

ElyCA project

Platform	Linux / BSD
License	**GPL**
Homepage	www.elyca.org
Download	
tar.gz	sourceforge.net eGroupWare project

firewall builder

Platform	Linux / BSD/ Mac
License	**GPL**
Homepage	www.fwbuilder.org
Download	
RPM	fwbuilder project
DEB	Debian project
tar.gz	fwbuilder project

fwlogwatch

Platform	Linux / BSD/ other
License	**GPL**
Homepage	fwlogwatch.inside-security.de
Download	
RPM	fwlogwatch project
DEB	fwlogwatch project
tar.gz	fwlogwatch project
tar.bz2	fwlogwatch project

logwatch project

Platform	Linux / BSD/ other
License	**GPL**
Homepage	www.logwatch.org
Download	
RPM	logwatch project
tar.gz	logwatch project

logcheck project

Platform	Linux / BSD/ other
License	**GPL**
Homepage	sourceforge project page
Download	
tar.gz	logcheck project

ModSecurity

Platform	Linux / BSD / WIN / other
License	**GPL**
Homepage	www.modsecurity.org
Download	
tar.gz	ModSecurity project
zip	ModSecurity project

NMAP

Platform	Linux / BSD / WIN / other
License	**GPL**
Homepage	www.nmap.org
Download	
RPM	NMAP project
tar.gz	NMAP project
tar.bz2	NMAP project
zip	NMAP project

OpenSSH project

Platform	Linux / BSD
License	**GPL**
Homepage	www.openssh.org
Download	
RPM	OpenBSD project fileserver
tar.gz	OpenBSD project fileserver

Osiris project

Platform	Linux / BSD/Win/Mac
License	**GPL**
Homepage	osiris.shmoo.com
Download	
tar.gz	Osiris project
Win EXE	Osiris project

PHP project

Platform	Linux / BSD / WIN /other
License	The PHP License
Homepage	www.php.net
Download	
RPM	Take a look at your distribution
tar.gz	php project
tar.bz2	php project
zip	php project

Rootkit Hunter

Platform	Linux / BSD / Mac
License	GPL
Homepage	http://www.rootkit.nl/projects/rootkit_hunter.html
Download	
RPM	packages external build
tar.gz	rootkit hunter homepage

Roxen web server project

Platform	Linux / BSD /WIN / other
License	**GPL**
Homepage	www.roxen.com/products/web server
Download	

The Linux package will be installed with a shell script

Shorewall		
Platform	Linux	
License	**GPL**	
Homepage	www.shorewall.net	
Download		
RPM		take a look at your distribution
DEB		Debian project
tar.gz		shorewall project

12 Useful Documentation

Open Source Development with CVS

Platform	All
License	**GPL**
Format	PDF
Homepage	http://cvsbook.red-bean.com/OSDevWithCVS_3E.pdf

Advanced Bash Scripting Guide

Platform	All
License	**Open Publication License**
Format	PDF / HTML
Homepage	http://www.tldp.org/LDP/abs/abs-guide.pdf

13 Example configuration scripts

13.1 AIDE

AIDE, Advanced Intrusion Detection System cron script

http://egroupware.org/scripts/aide_cronjob

md5sum d79a50428563764fea29f1c604f5d838

AIDE, sample config file

http://egroupware.org/scripts/aide.conf

13.2 Backup

MySQL backup cron script

http://egroupware.org/scripts/mysql_backup_cronjob.sh

md5sum e9902eb3303665dbdc6c8cb654c51e0f

PostgreSQL backup cron script

http://egroupware.org/scripts/postgresql_backup_cronjob.sh

md5sum b067023f0cec4ae09676c538524256e3

13.3 Iptables

Simple iptables firewall script (example from this document for advanced users)

http://egroupware.org/scripts/advanced_user_egroupware_iptables.sh

md5sum 3244f125e811e79c7a618231dc6a497f

Advanced Iptable firewall script

English version

http://egroupware.org/scripts/egroupware_iptables.sh

md5sum ee87dc2718c99057f1a4ffe76c2b73f2

Portuguese version

http://egroupware.org/scripts/br_egroupware_iptables.sh

md5sum 06284428564e69e7486d5f609c19104b

14 To-do and Change Log

14.1 The to-do list for this document

For document version 0.6:

- MaxDB
- Snort-inline
- Training the users
- Greylisting for mailservers
- Customisation the eGroupare
- Where to install the groupware
- Osiris installation and cutomization
- Firewall logwatch installation and usage
- Pre-planning an eGroupWare installation
- SMTP server installation and configuration
- IMAP / POP server installation and configuration
- Anti Virus and Spam protection for mail server/gateways
- Connect the Road warrior to the groupware (OpenVPN)

For document version 0.7:

- Windows/Mac extensions
- Setup and config the ElyCA certificate authority
- Tuning MySQL installation
- Installing an LDAP server and configuring OpenLDAP / Email / SMTP under *nix.
- Netscape Directory Server
- Netscape Certificate Management System

More after this release:

- mod_log_forensic for Apache.
- Hide the ssh version.
- Fedora support (YUM, RPM-apt).
- Add psad to the security HOWTO.
- sXad installation and config.
- Bastille Linux / LSAD.

14.2 Change log for the book

*** Sun Dec 05 2004 Reiner Jung <rjung AT expl0it DOT de> 0.5**

- fix error in Files restriction for Apache (Security)
- Aide example config file
- When you should update
- Troubleshooting extended
- Install eGroupWare with bitrock installer
- cvs update to the stable branch
- The filesystem layout from your server
- Restrict access to setup
- Firewall
  - Planing a firewall
  - How to create firewall rules
  - Example firewall script
  - Install the firewall script
  - Firewall logfile analyse
  - Example firewall script for download
- Config files for download
- Backup and restore your database
  - Decide your backup solution
  - Manually backup the MySQL database
  - Backup MySQL with a daily cronjob
  - Restore your MySQL database
  - MySQL backup script for download
  - Manually backup the PostgreSQL database
  - Postgresql backup script
  - Create a cron job for PostgreSQL
  - Restore your PostgreSQL database
  - PostgreSQL backup script for download
- Install eGroupWare with Bitrock Windows installer

*** Thu May 18 2004 Reiner Jung <r.jung AT creativix DOT net> 0.4**

- License changed to creative commons
- Build SuSE packages from source RPM
- Apache Security and Optimisation
- SQL encryption for user password possible
- Setup provides account prefix for LDAP installations
- Select in setup case sensitive usernames
- Troubleshooting added
- Secure your eGroupWare with ModSecurity
- update the header.inc.php file
- Secure PHP installation updated

open basedir restriction

disable error logs

- Setup Advanced Intrusion Detection System
- Change the Quick install HOWTO to Express Install HOWTO and extend it
- Express Install includes Windows now
- Install logfile analyser (logcheck)
- Turck-mmcache extended

How to install mmcache on RedHat Enterprise Linux

Requirements for install mmcache

*** Sun Nov 22 2003 Reiner Jung <r.jung AT creativix DOT net> 0.3**

- Update eGroupWare

Update with packages

Update from CVS

- Install from a RPM to a other path like /var/www/html
- Software Map

Add the software and the license from all pieces from 03 documents

- Some typo errors fix

GPG key typo fixed

- Verify the GPG key added
- Create a https certificate
- Secure PHP installation

*** Fri Sep 16 2003 Reiner Jung <r.jung AT creativix DOT net> 0.2**

- Some typo errors fixed

Fix error in CVS install documentation and in mmcache

- chkrootkit how to added

Checkrootkit sample snippet

Install check rootkit RPM

Install check rootkit tar.gz

- check your server for unneeded service / open ports

Ports which eGW server needs to run

The portscanner

Output from the portscanner

Disable unneeded services/servers

- uninstall unneeded software extended
- secure administration (ssh/sshd)

Connecting your server with a secure session

Working with ssh key pairs

Creating a secure shell key pair

Copying your public key to the server

The ssh-add tool , Securing your ssh client

Securing your sshd

15 Contributors to this Document

The following people have contributed to the Install and Security HOWTO:

Translations

Brazil Portuguese:	Roger de Souza Moraes, Leandro Arruda, Renato Cintra, Tales Costa
French:	Patrice Lallement (v0.3)
Spanish:	Oscár Manuel Gómez Senovilla
Indonesian:	Willy Sudiarto Raharjo
Traditional Chinese:	Finjon Kiang

Proof reading

English:	Jeff Mitchell (v0.4, 0.5)
	Geltmar von Buxhoeveden (v0.3)

Co-Authors

Windows Version	John W. Brown

Artwork and Prepress Andreas Krause

16 Humanly-Readable License

Attribution-ShareAlike 2.0

You are free:

- to copy, distribute, display, and perform the work
- to make derivative works
- to make commercial use of the work

Under the following conditions:

Attribution. You must give the original author credit.

Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under a license identical to this one.

- For any reuse or distribution, you must make clear to others the license terms of this work.
- Any of these conditions can be waived if you get permission from the author.

Your fair use and other rights are in no way affected by the above.

This is a human-readable summary of the Legal Code (the full license) [26].

26 http://creativecommons.org/licenses/by-sa/2.0/legalcode

17 Index

Errata: