

Quartz Manual

V 1.00

October 27, 2005
UCSB

Installation and user initialization	3
Setup of groups and files	4
Adding Files	
Removing Files	
Synchronization of files	5
File Storage	
File Updates	
User interface	7
Command List	
Displaying all Information	
Troubleshooting	8
Encryption/Decryption Issues	
System Corruption	
Stolen Device or Password	

Installation and user initialization

Once you have downloaded the tar ball of Quartz, untar the file from the folder in which you would like Quartz to be installed off of. Then, change into the Quartz directory and simply type the command `./install` in order to create the executable and move all necessary system files into the “quartz” directory.

```
ucsb% tar -xzvf quartz_v_1_00.tgz
ucsb% cd quartz
ucsb% ./install
```

Quartz will prompt the user to setup his user information the first time Quartz is executed on a particular device. In this time, the user is able to register a new alphanumeric username within the Quartz network along with an alphanumeric password of length 7-12. Also, the user is able to create or recreate their symmetric private key based on the provided password. Physically copying one particular key throughout all the user’s devices is necessary for encryption and decryption of all their files – do not use separate keys even though they may be generated from the same password.

A terminal window titled "Terminal" showing the output of the Quartz installation script. The script prompts for user information and displays the resulting configuration. The user enters 'MrQuartz' as the username, 'peertopeer' as the password, 'mattsun@cs.ucsb.edu' as the email address, 'laptop' as the node name, and '128.111.40.228' as the IP address. The script confirms the information, registers the user, and generates an RSA private key. The terminal output is as follows:

```
Terminal
File Edit View Terminal Tabs Help
SETTING UP QUARTZ! v1.0
*****
You have not setup user information for this device.
Please enter the following information:

Username: MrQuartz
Password:
Email Address [mattsun@cs.ucsb.edu]:
Node name [bishop]: laptop
IP Address [128.111.40.228]:

You entered the following information:

USER INFORMATION
-----
NAME = mrquartz
PASSWORD = peertopeer
IDENTITY HASH = 8AD3E8357FB0BA888E381A148F3290A0F
EMAIL = mattsun@cs.ucsb.edu
NODE = laptop
IP ADDRESS = 128.111.40.228
-----

Is this information correct? [yN] y
Are you already registered with Quartz? [yN] n
Would you like to register with Quartz? [yN] y
Username "mrquartz" has been successfully registered!
Saving user information... done

Recreating key in "./key"
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)

Either copy this key over to all your other
devices or replace this one with your used key.

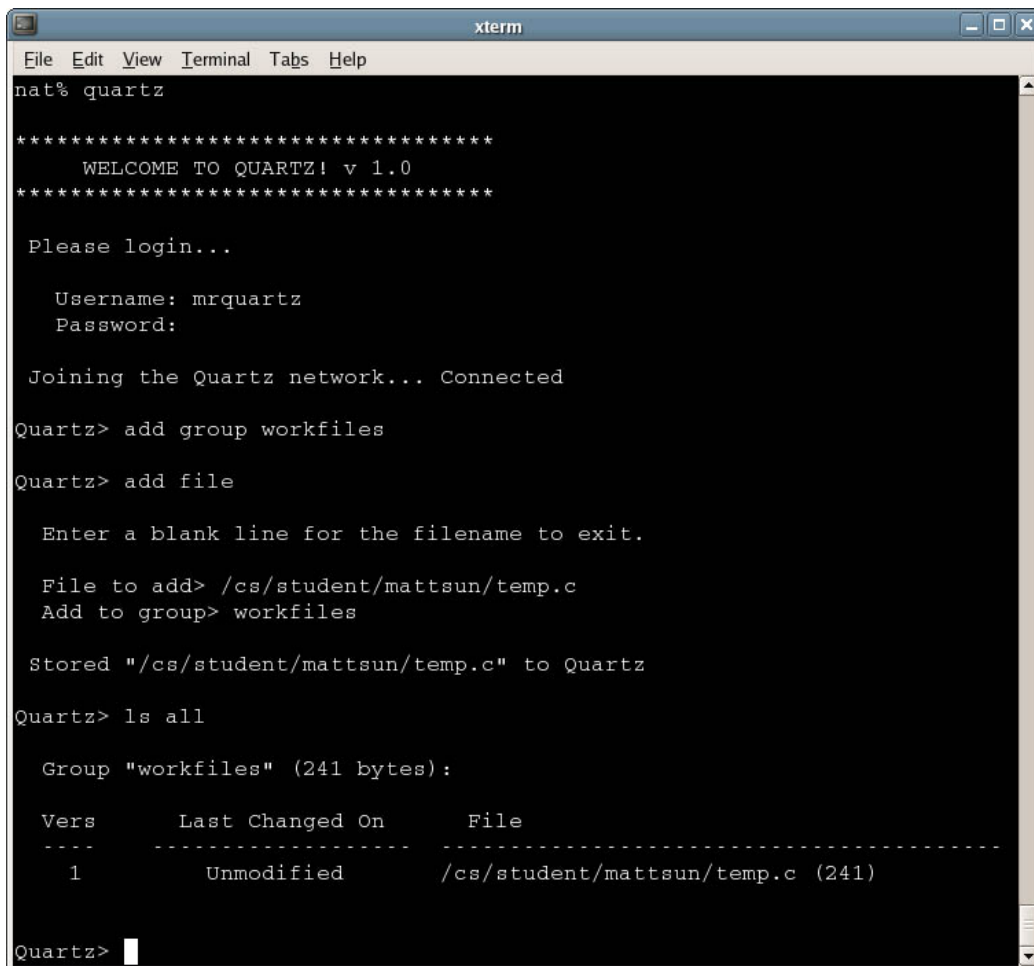
You are now setup to run Quartz!
Please run "quartz" again. Thank you.
bishop%
```

At this point, Quartz is properly setup. Quartz automatically quits from setup in order to allow the user to either copy the newly created key amongst all their devices or to copy over a previously created key, rewriting the one just constructed. To sign on and connect to the Quartz network, the user executes `quartz*` and signs on by correctly inputting a registered username and password.

Setup of groups and files

Adding Files/Groups

Quartz synchronizes files by setting up groups. Each group characterizes those files that the user wants to keep synchronized distinct from other possible groups. For example, if a user wants to keep their files concerning a webpage synchronized among their devices, the user could add a group titled “webpage.” Then the user is able to add any number of files that comprise the entire webpage, including all necessary html files. There are two provided ways of adding new groups, depending on the preferred choice. One way is to type ``add group [name of group]``. The other way is to type ``add group`` where the system will prompt you to enter any number of groups. To stop adding a group or cancel altogether, press enter (input an empty group name).



```
xterm
File Edit View Terminal Tabs Help
nat% quartz
*****
WELCOME TO QUARTZ! v 1.0
*****

Please login...

Username: mrquartz
Password:

Joining the Quartz network... Connected

Quartz> add group workfiles

Quartz> add file

Enter a blank line for the filename to exit.

File to add> /cs/student/mattsun/temp.c
Add to group> workfiles

stored "/cs/student/mattsun/temp.c" to Quartz

Quartz> ls all

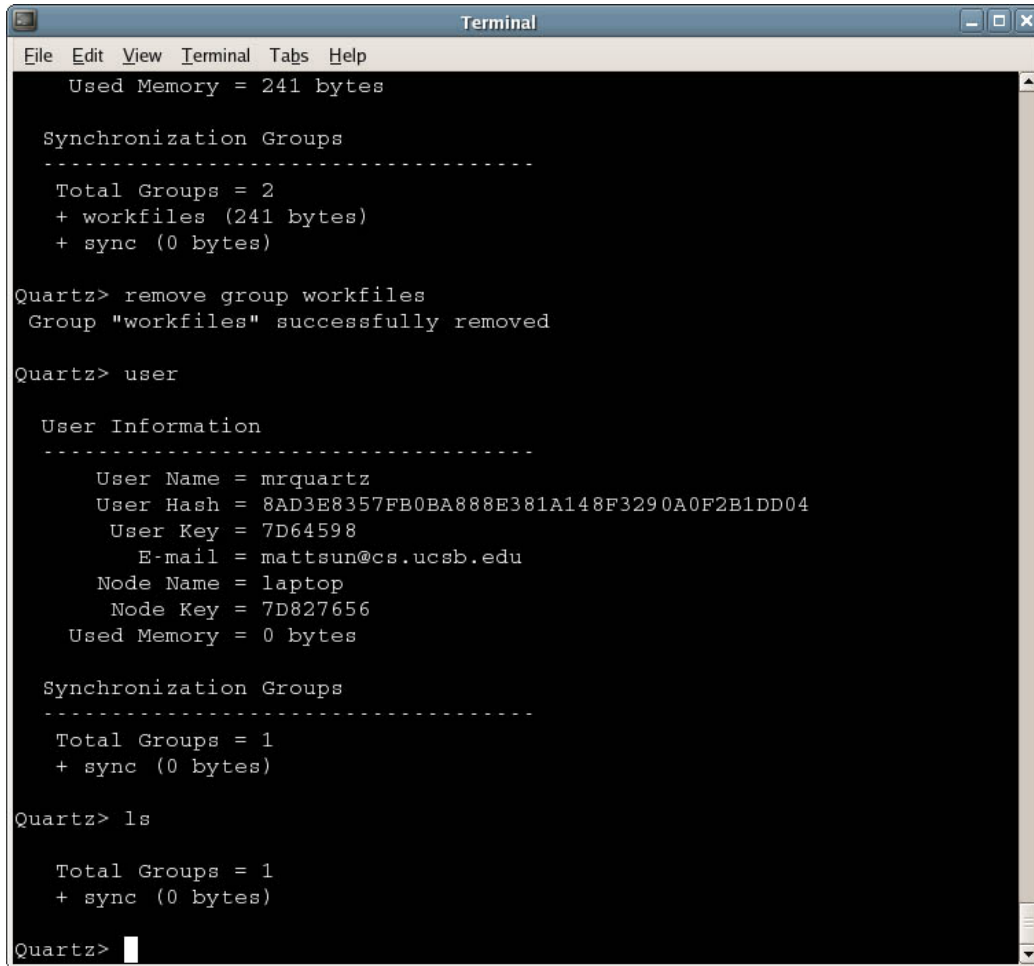
Group "workfiles" (241 bytes):

Vers      Last Changed On      File
-----
1          Unmodified           /cs/student/mattsun/temp.c (241)

Quartz>
```

Removing Files/Groups

Removing groups follows the same syntax as adding. If a user wants to remove a particular file from a group, they would type ``remove file``. From this point on, Quartz will ask you what file to remove and from what group. Again, the user is able to `<tab>` the filename, making sure that file exists on the hard drive. This will not delete the file on the local hard drive. It will, instead, remove the file from being stored on the network and peers themselves. If a user wants to remove an entire group and all the files it consists of on the network, the user would type ``remove group <group name>``.



```
Terminal
File Edit View Terminal Tabs Help
Used Memory = 241 bytes

Synchronization Groups
-----
Total Groups = 2
+ workfiles (241 bytes)
+ sync (0 bytes)

Quartz> remove group workfiles
Group "workfiles" successfully removed

Quartz> user

User Information
-----
User Name = mrquartz
User Hash = 8AD3E8357FB0BA888E381A148F3290A0F2E1DD04
User Key = 7D64598
E-mail = mattsun@cs.ucsb.edu
Node Name = laptop
Node Key = 7D827656
Used Memory = 0 bytes

Synchronization Groups
-----
Total Groups = 1
+ sync (0 bytes)

Quartz> ls

Total Groups = 1
+ sync (0 bytes)

Quartz> |
```

Synchronization of files

All groups and files will be synchronized with a simple ``sync`` command in order to minimize any complications and confusions. Single files can be synchronized individually, or groups can be synchronized all at once. In the case that a more recent version of a file exists within the network, Quartz will ask the user whether or not they want to update that particular file. If not, the user is still asked if they want to store that version of the file as the newest within the network. If a request is made to synchronize the entire group, existing files will behave exactly the same; however, new files detected

that did not previously exist within a device will be automatically added to a user's local directory (with subdirectories created when necessary). For example, a user on one device creates a group "huge" and adds 10 files to the group that they recently edited. The user is able to go to their other device, add the group "huge" and type ``sync huge`` in order to automatically update/create all 10 files residing on the Quartz network. When a particular file is requested to be synchronized, and that file is the most recent version, the file will be stored within the network only if it has been updated (by comparing modification time stamps from the file system) since its previous synchronization/update.

```

Terminal
File Edit View Terminal Tabs Help
User Name = mrquartz
User Hash = 8AD3E8357FB0BA888E381A148F3290A0F2B1DD04
User Key = 7D64598
E-mail = mattsun@cs.ucsb.edu
Node Name = laptop
Node Key = 7D827656
Used Memory = 0 bytes

Synchronization Groups
-----
Total Groups = 2
+ workfiles (0 bytes)
+ sync (0 bytes)

Quartz> sync workfiles

Synchronizing group "workfiles"...

New file detected from Quartz!
Adding: file "/local/home/mattsun/temp.c" to group "workfiles"

Quartz> Decrypting... done! Updated "/local/home/mattsun/temp.c"

Quartz> ls group workfiles

Group "workfiles" (241 bytes):

Vers      Last Changed On      File
-----
1          Unmodified           /local/home/mattsun/temp.c (241)

Quartz>

```

File Storage

Using the sync command, Quartz stores files onto the network in several cases. The file of a given group must be of the most recent version stored already and that file must be modified since its last synchronization. Also, although the user may not have the most recent version, they may force store that file by following the given prompts by the system. The last way Quartz will store files onto the network is if it is a new file not previously added to the group. The user will detect that the file is not currently stored within Quartz and will automatically store the encrypted file for you.

File Updates

Quartz updates your files from the network in several cases. If a sync command is performed on a particular file (or group) and that file is not the most recent version stored within Quartz, you will be asked to update that file. Also, if your group currently lacks one or more files that are stored as part of that particular group within the network, a sync command on that group will automatically create those file(s). In addition, if any number of subdirectories pertaining to that file does not exist, Quartz will automatically create those for you.

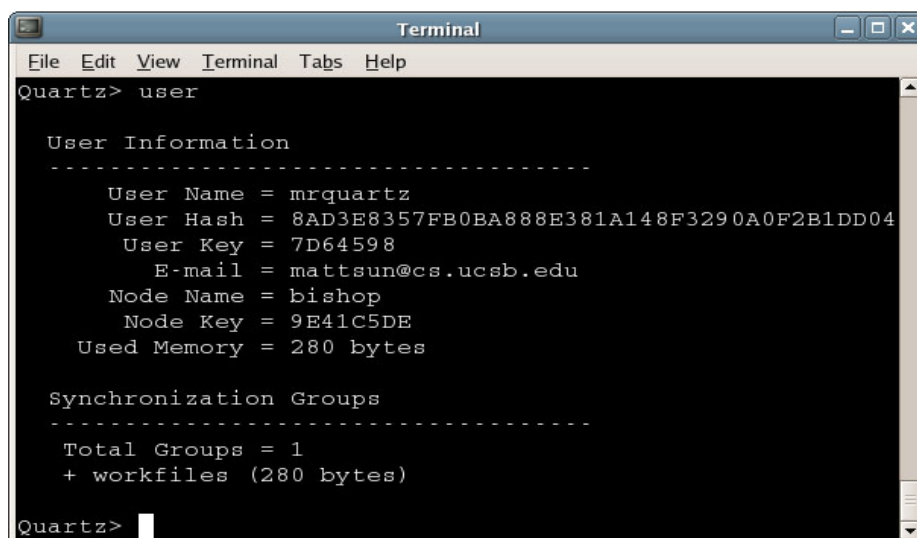
User interface

Command List

In order to view all commands allowed, the user can type ``help`` and a list of commands will be shown. If the user does not know how to use a particular command from that list, the user can type ``[command] help`` to show proper usage of the given command. The `Quartz>` prompt acts like a normal command prompt in that it records a history of previously used commands as well as the `<tab>` feature that can find and “complete” file names existing on the local device.

Displaying all Information

To view all of your user information that Quartz takes into account, the user must either type ``show user`` or ``user``, depending on their preference. To view just the names of the groups and their total memory usage, the user can type ``show groups`` or ``ls`` in order to imitate normal command prompt behavior once again. If the user types ``show all groups`` or ``ls all``, each group, all of their files, and each file’s associated sizes and their status are listed. The status refers to whether or not the file has been updated from Quartz and if it has been modified since its last synchronization (through the modification time stamp).

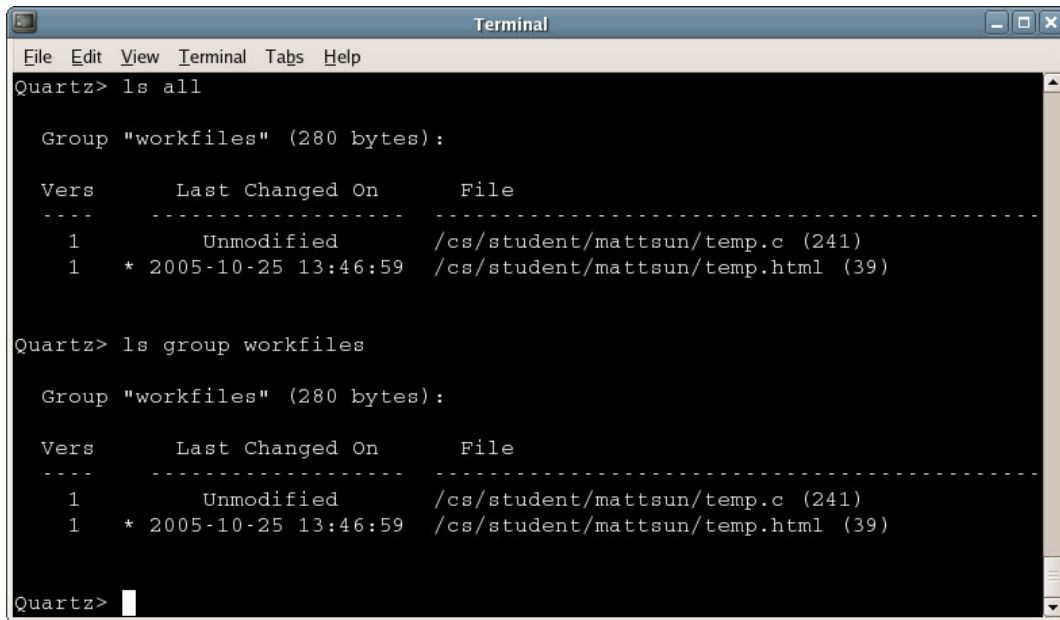


```
Terminal
File Edit View Terminal Tabs Help
Quartz> user

User Information
-----
User Name = mrquartz
User Hash = 8AD3E8357FB0BA888E381A148F3290A0F2B1DD04
User Key = 7D64598
E-mail = mattsun@cs.ucsb.edu
Node Name = bishop
Node Key = 9E41C5DE
Used Memory = 280 bytes

Synchronization Groups
-----
Total Groups = 1
+ workfiles (280 bytes)

Quartz> |
```



```
Terminal
File Edit View Terminal Tabs Help
Quartz> ls all

Group "workfiles" (280 bytes):

Vers      Last Changed On      File
-----
1          Unmodified           /cs/student/mattsun/temp.c (241)
1 * 2005-10-25 13:46:59 /cs/student/mattsun/temp.html (39)

Quartz> ls group workfiles

Group "workfiles" (280 bytes):

Vers      Last Changed On      File
-----
1          Unmodified           /cs/student/mattsun/temp.c (241)
1 * 2005-10-25 13:46:59 /cs/student/mattsun/temp.html (39)

Quartz> |
```

In the above example, file “temp.c” will not be stored within the network if that device already has the most recent version and the user performs a sync on that file, because its status is not modified. On the other hand, file “temp.html” will be stored within the network, because it has been modified (with the listed date) since its last synchronization.

Troubleshooting

Encryption/Decryption Issues

When encrypting a file upon storage onto the network, if it says “Unable to load private key”, make sure that, first, the key exists within the same directory and, second, that your password is the same used when creating the key to begin with (possibly on another device).

When decrypting an updated file, if an error appears describing padding issues, this means that you have not yet copied over the shared private key that was used to encrypt the file to begin with. Make sure that you have copied over the same key over to all of your devices under the same username and password.

System Corruption

If any of the .qtz system files get corrupted, remove *.qtz and rerun Quartz. The user will be prompted to setup its user information once again. Using the same username and password, the user is still able to retrieve all of their files. Because Quartz is still in one of its first release phases, it may not be as stable as we would like – in other words, perfection. If Quartz crashes or is inoperable at any moment, please quit the program

either by typing `quit` or by hitting Ctrl+C and e-mail the file my.log over to us at mattsun@cs.ucsb.edu with the subject “[quartz] log”.

Stolen Device or Password

If someone steals a device, and you are worried of them obtaining and corrupting the files you have currently stored on the Quartz network, remember that the user is unable to join the network unless they have the correct password. Even bypassing the password prompt screen through whatever hacking methods may be used, the attacker still would not be able to decrypt those files because the private key can only be opened with the correct password. If someone attains your password, you can change your password only by sending a request to mattsun@cs.ucsb.edu with the subject “[quartz] password” using the same e-mail address you used to register your username to begin with. The e-mail address must match that stored originally by Quartz. Our server will simply remove your entire user entry from the registry so that you may once again re-register your username and a new password. It is important to keep your username the same, because synchronization of those files currently residing within Quartz is based on the user’s name. Again, if you want to change/update that registered e-mail address, please send yet another request to mattsun@cs.ucsb.edu with the subject “[quartz] email” with your new e-mail address being the only text in the message.