SimpleRisk LAMP Installation Guide

Introduction

SimpleRisk is a simple and free tool to perform risk management activities. Based entirely on open source technologies and sporting a Mozilla Public License 2.0, a SimpleRisk instance can be stood up in minutes and instantly provides the security professional with the ability to submit risks, plan mitigations, facilitate management reviews, prioritize for project planning, and track regular reviews. It is highly configurable and includes dynamic reporting and the ability to tweak risk formulas on the fly. It is under active development with new features being added all the time and can be downloaded for free or demoed at http://www.simplerisk.org.

Disclaimer

The lucky security professionals work for companies who can afford expensive GRC tools to aide in managing risk. The unlucky majority out there usually end up spending countless hours managing risk via spreadsheets. It's cumbersome, time consuming, and just plain sucks. When Josh Sokol started writing SimpleRisk, it was out of pure frustration with the other options out there. What he's put together is undoubtedly better than spreadsheets and gets you most of the way towards the "R" in GRC without breaking the bank. That said, humans can make mistakes, and therefore the SimpleRisk software is provided to you with no warranties expressed or implied. If you get stuck, you can always try sending an e-mail to support@simplerisk.org and we'll do our best to help you out. Also, while SimpleRisk was written by a security practitioner with security in mind, there is no way to promise that it is 100% secure. You accept that as a risk when using the software, but if you do find any issues, please report them to us so that we can fix them ASAP.

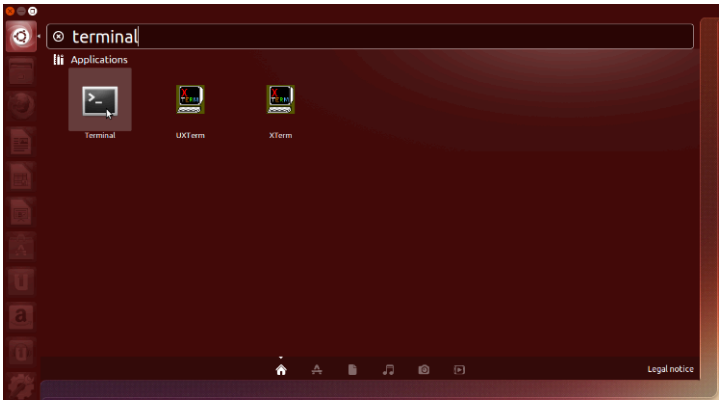
Install Ubuntu

SimpleRisk should be able to work on just about any operating system that is capable of running PHP and MySQL. Since the purpose of this guide is to get you up and running with SimpleRisk as quickly as possible, we assume that you are using Ubuntu, a FREE and easy to use Linux-based operating system. Download the latest version of Ubuntu (at the time of this writing it's 13.04) and install it. See the Ubuntu documentation if you are having any issues there. Once you have a working installation, you can move on to the next installation steps.

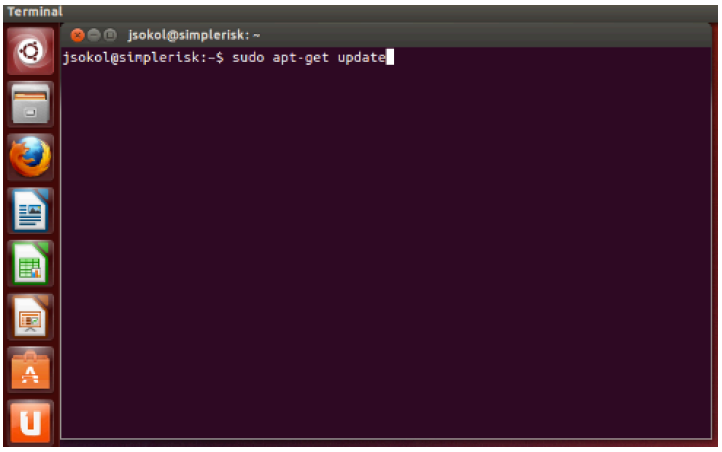
Get the Latest Ubuntu Updates

Log in to your Ubuntu installation using the username and password you defined at setup. Select the Unity menu (the one at the very top of the bar on the left) and type "terminal" in the field that pops up. This should show you a shortcut to the terminal application. You can click it to launch the terminal, but

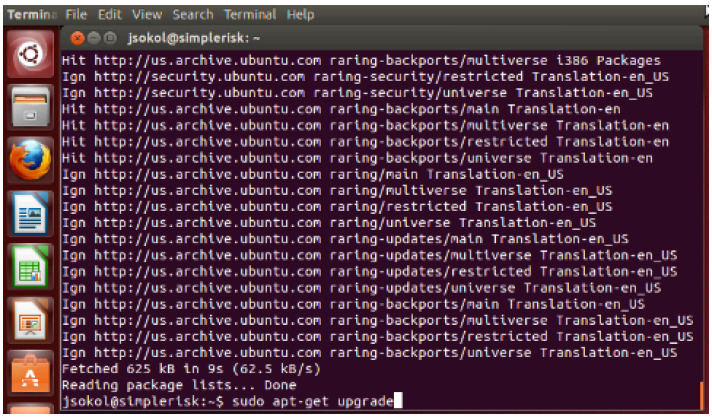
it may be a good idea to drag it to the Unity bar on the left first so that you can easily start it in the future.



Once the terminal is launched, you will want to update the OS to the latest software versions available. To do this run “sudo apt-get update” and enter your password when prompted.

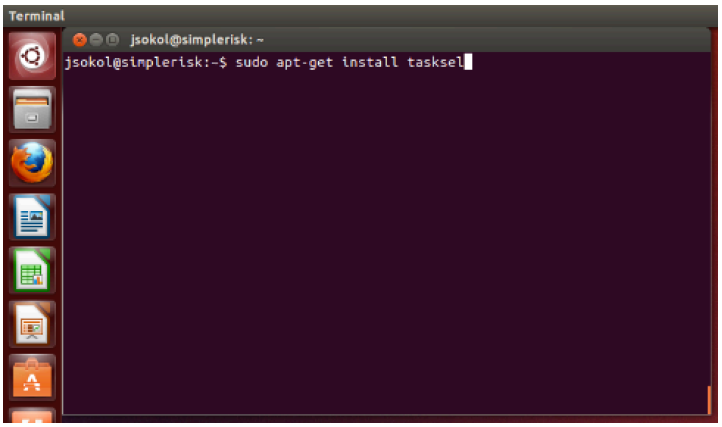


This will pull down the latest version information for all of the installed operating system files. Now run “sudo apt-get upgrade” and answer “y” when it asks if you would like to continue.

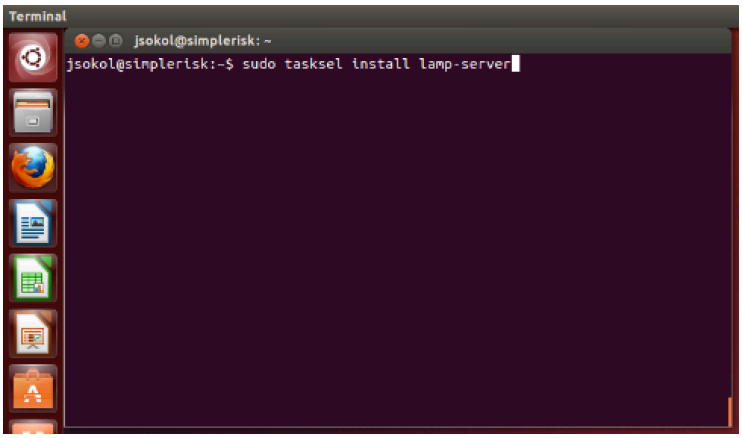


Installing Apache, PHP, and MySQL

The next step is to install the necessary files in order to run Apache with PHP and MySQL on this system. To do, this first run the command “sudo apt-get install tasksel”.



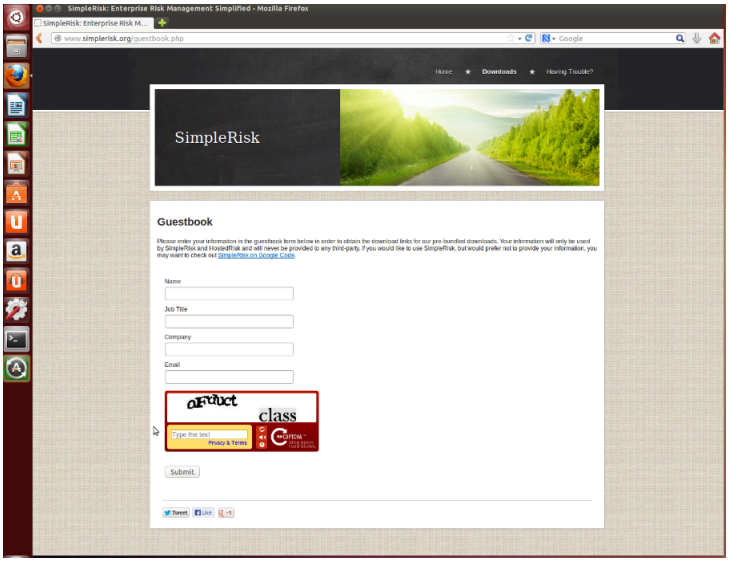
Next, tell the server to install a LAMP stack by running the command “sudo tasksel install lamp-server”.



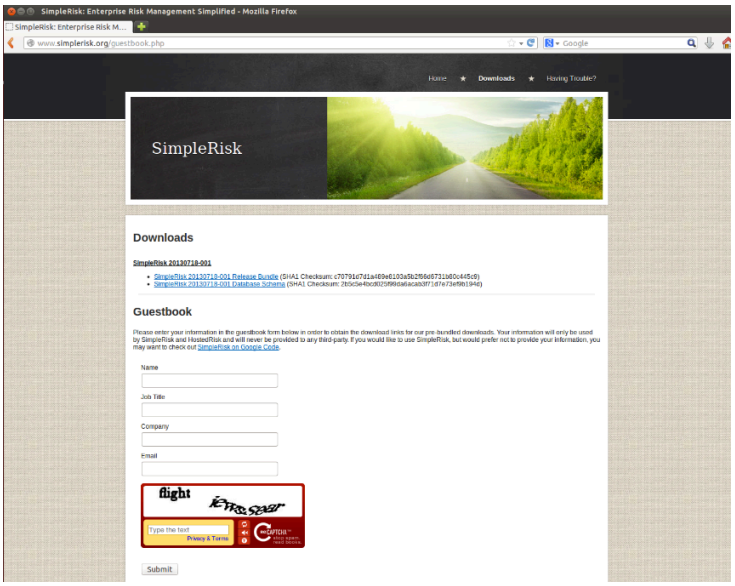
You should now see the terminal change into a package configuration application that downloads and installs the applications necessary in order to run a LAMP stack on the server. Eventually it will pause the install in order to ask you to specify a MySQL “root” password. Generate a long and random password and save it off in a secure location so that you can access it later. You will know that this installation process is complete when the package configuration screen goes away and you are back at the terminal shell.

Obtaining the SimpleRisk Files

Click on the FireFox logo in the Unity bar on the left. Once FireFox loads, enter http://www.simplerisk.org into the URL bar to go to the SimpleRisk site. Click on the “Downloads” link at the top. Then, select the link on the downloads page to obtain the “Latest SimpleRisk Release Bundle”.



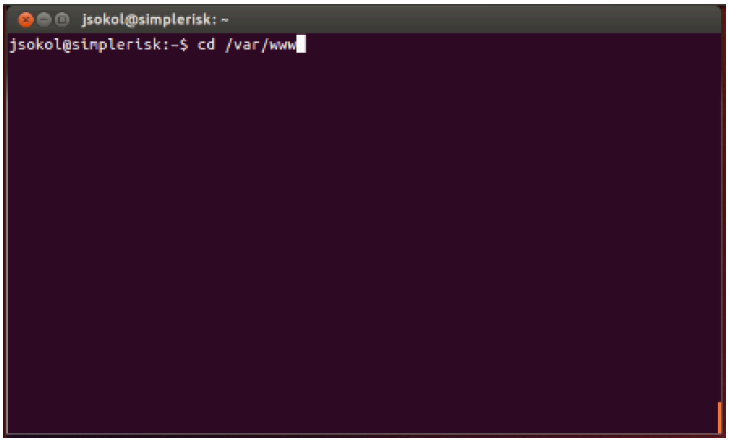
Enter your name, job title, company, and e-mail address into the SimpleRisk guestbook. Your information will never be sold to another party. We only keep this data so that we can keep you updated on the latest application and security updates for the tool. Complete the CAPTCHA and click the "Submit" button. If it was successful, the page should update with a link to the downloads on the page.



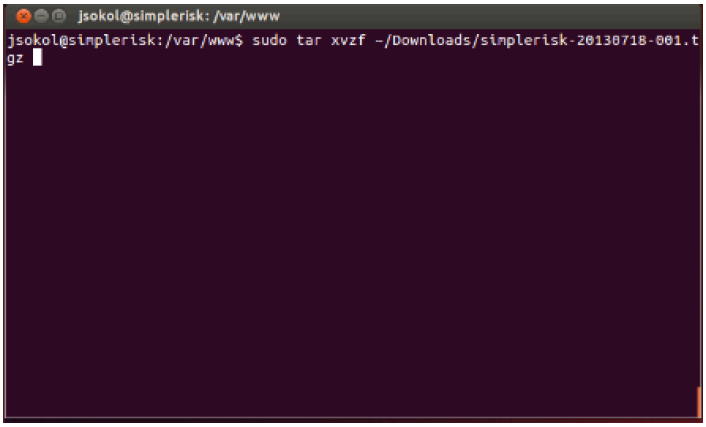
Click to download and save both the latest release bundle and the associated database schema. Once you have the files downloaded, you can close the browser.

Installing the Web Files

Change to the new Apache web root by running the command "cd /var/www".



Remove the default index page using the command “sudo rm index.html”. Extract the web bundle into the web directory using the command “sudo tar xvzf ~/Downloads/simplerisk-20130718-001.tgz” (or whatever the most current version available is).



This will extract the files into a directory under the web root named “simplerisk”. You will need to access the files with a “/simplerisk” appended to the URL. Optionally, you can run the following commands to move it to the web root:

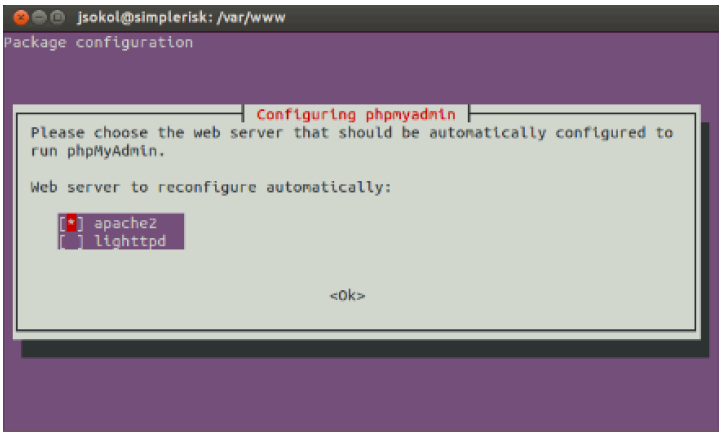
- sudo mv simplerisk/* .
- sudo rmdir simplerisk

Installing the Database

The hands-down easiest way to install the SimpleRisk database is to use something like PHPMyAdmin to create the new database and import the .sql file. We are going to install it just to make things easier on us, but will remove it later. Run the following command:

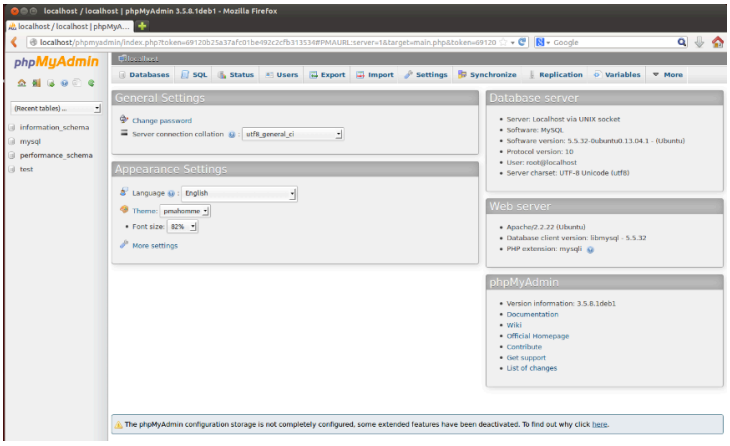
- sudo apt-get install phpmyadmin

When it prompts you to download the various files enter “y”. Eventually it will bring you to a screen to configure the phpmyadmin installation. Use the space bar to select the “apache2” web server configuration and then hit tab to move the cursor to OK and hit enter.

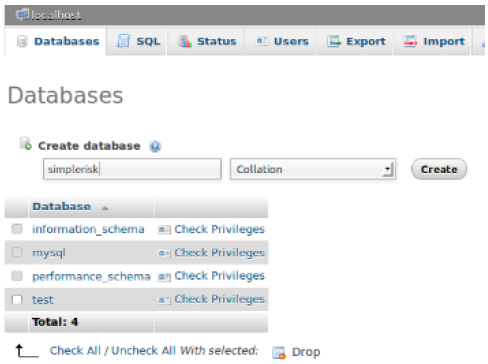


It will prompt you with a message about configuring the database. Hit enter to move past that. When it asks you to configure the database for phpmyadmin with dbconfig-common, hit tab to select no and then hit enter.

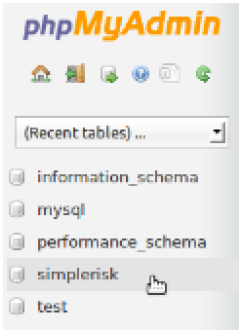
Open up FireFox again and enter http://localhost/phpmyadmin in the URL bar. Enter username “root” and then the password that you used when it prompted you during the LAMP stack installation up above. This should bring you into PHPMyAdmin. Click on the “Databases” tab at the top.



Tell it to create a database named “simplerisk” and click on Create.

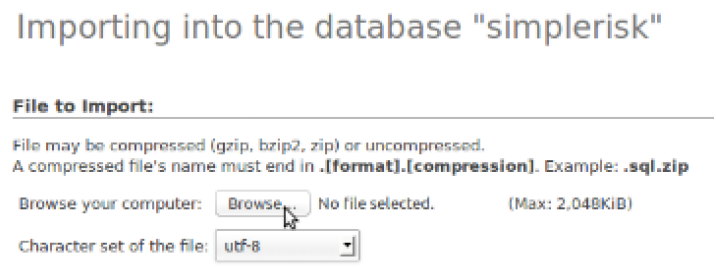


Select your new database from the menu on the left.

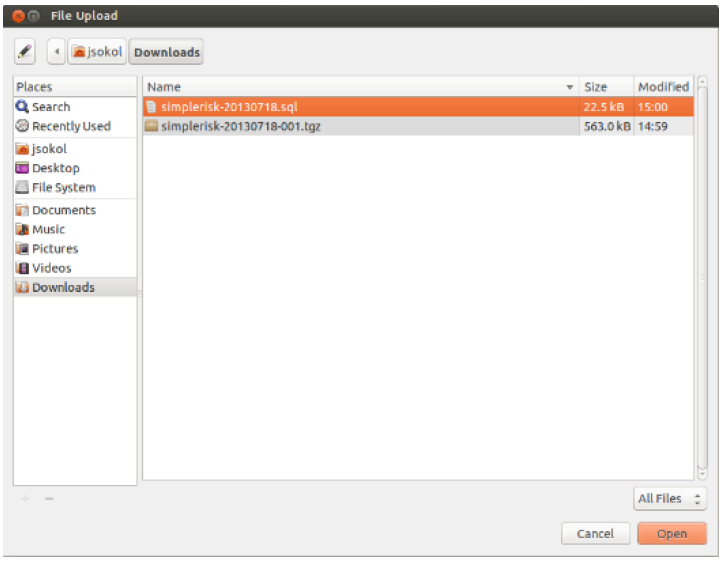


Click on the “Import” tab at the top.

Select “Browse” and browse to the database file which you downloaded earlier in this document.



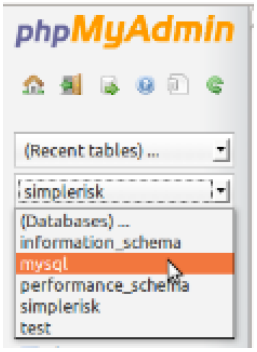
If you followed this document so far, then it should be in your “Downloads” folder.



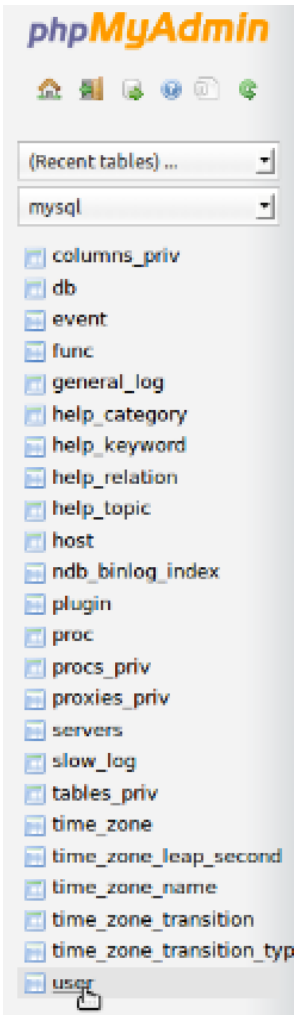
Click “Open” and then click “Go”.

Creating a Database User and Setting Permissions

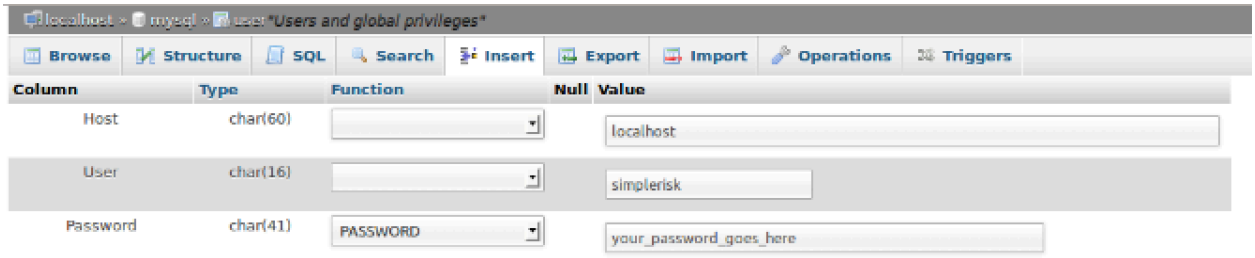
While still in PHPMyAdmin, select the “simplerisk” database name on the left and in the dropdown list select “mysql”.



Select the “user” table from the list of tables in the mysql database.

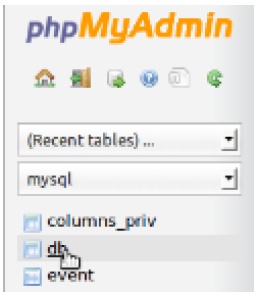


Select “Insert” from the tabs at the top. Put “localhost” in the Value field for the Host column. Put “simplerisk” in the Value field for the User column. Create a new random password and put it in the Value field for the Password column. Change the function in the Password column to “PASSWORD”. You can leave the privileges no for everything.



Scroll down towards the bottom of that insertion and select “Go” to add the new user. You may get some warning messages, but select “Browse” from the tabs at the top and you should see your new user in there.

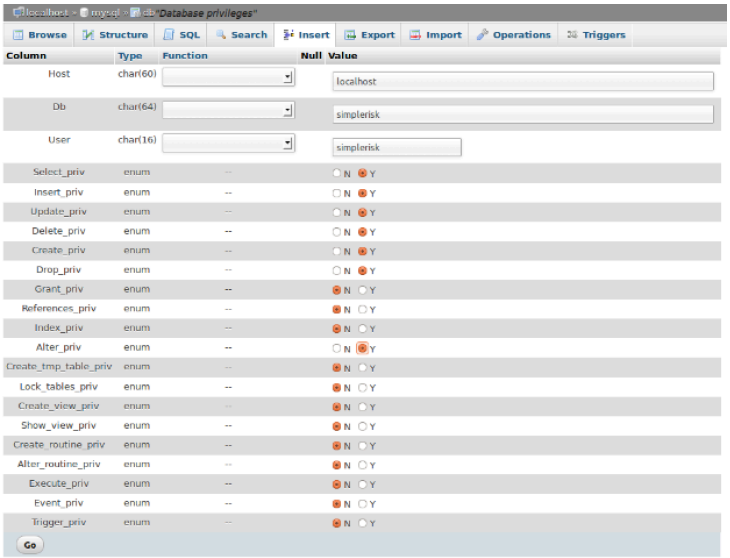
Select the “db” table from the list of tables in the mysql database.



Select “Insert” from the tabs at the top. Put “localhost” in the Value field for the Host column. Put “simplerisk” in the Value field for the Db column. Put “simplerisk” in the Value field for the User column. Change the following privilege values to “Y”:

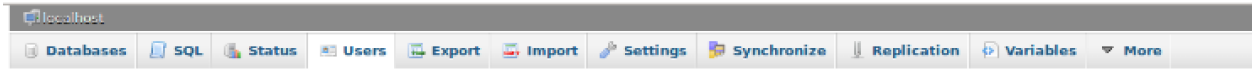
- Select_priv
- Insert_priv
- Update_priv
- Delete_priv
- Create_priv
- Drop_priv
- Alter_priv

SimpleRisk does not create, drop, or alter tables on a regular basis, but these permissions are necessary for upgrades. If you would like to set these to “N” for security reasons (least privilege), just remember that you may need to change them at a later point.

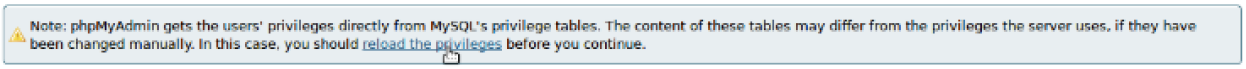


Click “Go” to add the entry. Select the “Home” button at the top left.

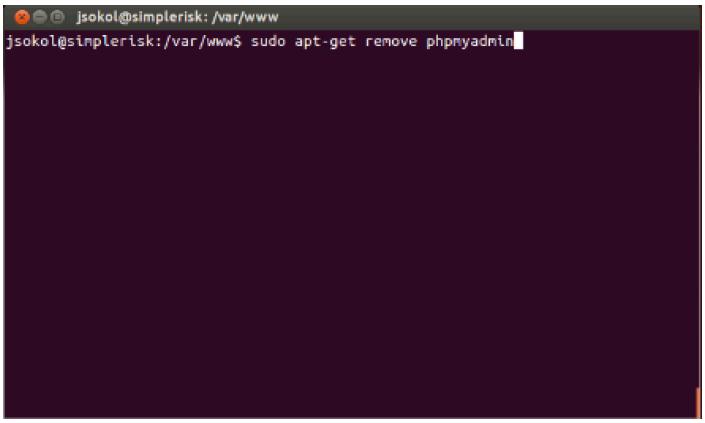
Select “Users” from the tabs at the top.



Click the link at the bottom of the page that says “reload the privileges”.

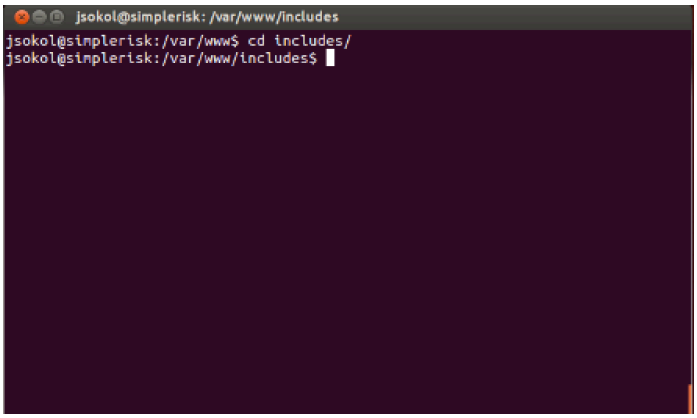


Close FireFox. Go back to the terminal and enter the command “sudo apt-get remove phpmyadmin”. Enter “y” when it asks if you would like to continue.



Connecting SimpleRisk to the Database

The last step in getting SimpleRisk installed is connecting the web files to the database. To do this, in the web directory, run the command “cd includes” if you followed the optional moving of the directory above or “cd simplerisk/includes” if you did not.

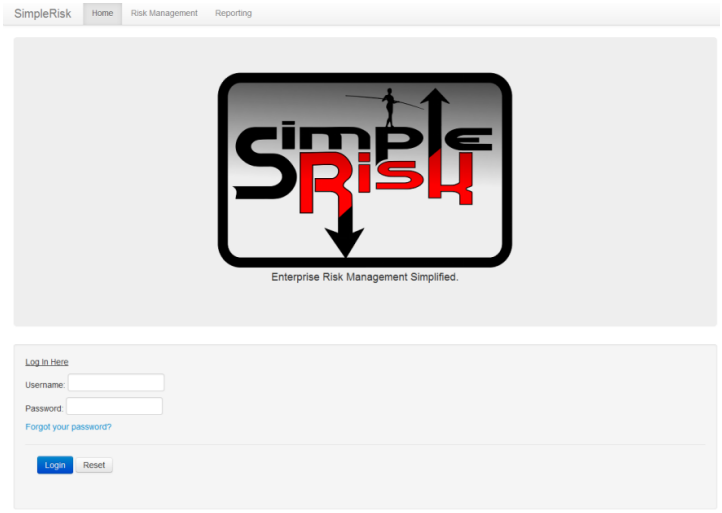


In the “includes” directory you will see a file named “config.php”. This is the configuration file for SimpleRisk. To edit the file, use the command “sudo pico config.php”. Change the DB_HOSTNAME value from “db_host” to “localhost”. Change the DB_USERNAME value from “db_user” to “simplerisk”.

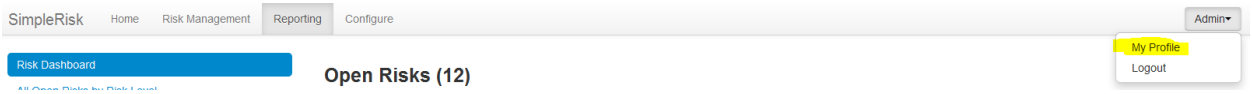
Change the DB_PASSWORD value from “db_pass” to the password you set for the simplerisk user in the step above. Change the DB_DATABASE value from “db_name” to “simplerisk”. There are also a couple of values that you can change in order to modify how long it takes for sessions to timeout and/or renegotiate. I suggest leaving the default values here. Lastly, you can change the timezone so that times are recorded based on wherever you are. The list of supported timezone values can be found at http://www.php.net/manual/en/timezones.php. Use ctrl + x to tell the editor you want to exit and enter “y” when it asks if you want to save the modified buffer. Then, just hit enter in order to overwrite the existing config.php file.

Logging in to SimpleRisk

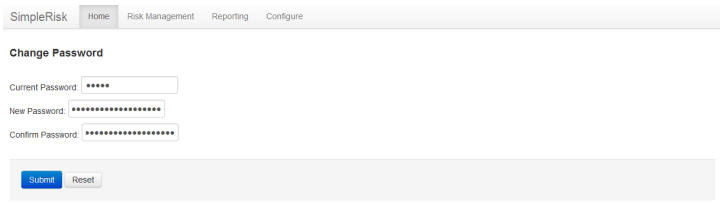
You should now have performed all of the steps you need to for SimpleRisk to be up and running. Now is the moment of truth where we hopefully get to see if all of your hard work paid off. You now need to point your web browser to the URL where SimpleRisk would be installed. If you followed the optional instructions, then it should be located at http://localhost/. If you did not, then it is probably located at http://localhost/simplerisk. You will know that you’ve got the right page when you see something like this:



Enter username “admin” and password “admin” to get started. Then, select the “Admin” dropdown at the top right and click on “My Profile”.



Enter your current password as “admin” and place a new long and randomly generated password into the “New Password” and “Confirm Password” fields. Then click “Submit”.



You should receive a message saying that your password was updated successfully. If so, then this is your new “admin” password for SimpleRisk. This completes your installation of SimpleRisk. Next you will want to check out the SimpleRisk Configuration Guide to determine if there are any configurations that you need to modify.