Install SimpleRisk on Ubuntu 18.04

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 https://www.simplerisk.it/.

Disclaimer

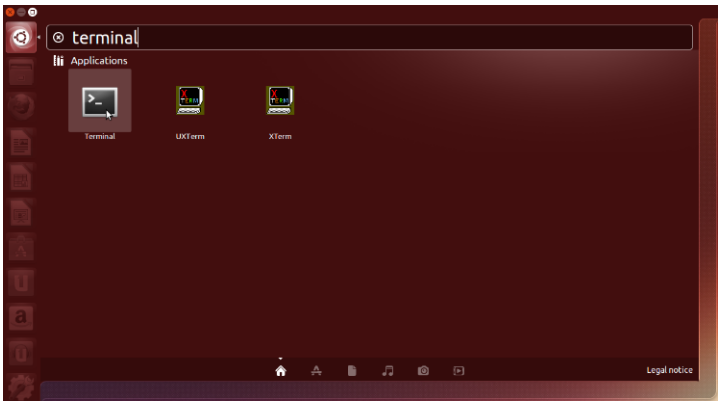
The lucky security professionals work for companies who can afford expensive GRC tools to aide in managing risk. The unlucky majority out there usually end up spending countless hours managing risk via spreadsheets. It's cumbersome, time consuming, and just plain sucks. When Josh Sokol started writing 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.it 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

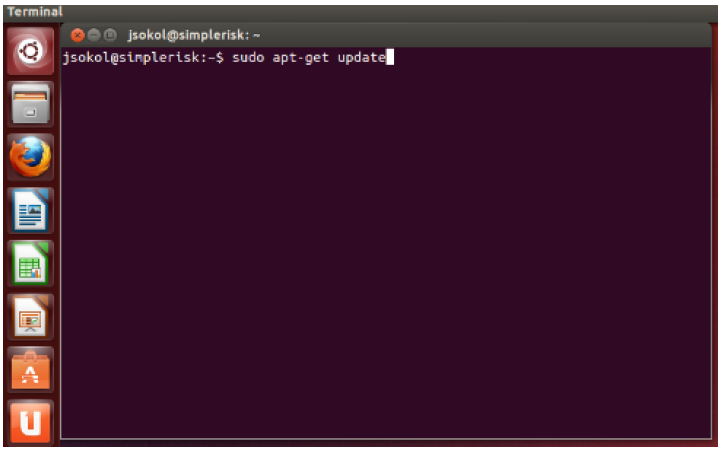
SimpleRisk should be able to work on just about any operating system that is capable of running PHP and MySQL. Since the purpose of this guide is to get you up and running with SimpleRisk as quickly as possible, we assume that you are using Ubuntu, a FREE and easy to use Linux-based operating system. Download the latest version of Ubuntu 18.04 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

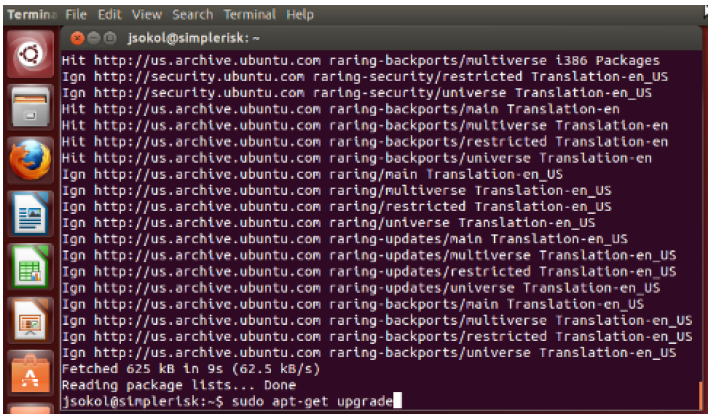
Log in to your Ubuntu installation using the username and password you defined at setup. Select the Unity menu (the one at the very top of the bar on the left) and type "terminal" in the field that pops up. This should show you a shortcut to the terminal application. You can click it to launch the terminal,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

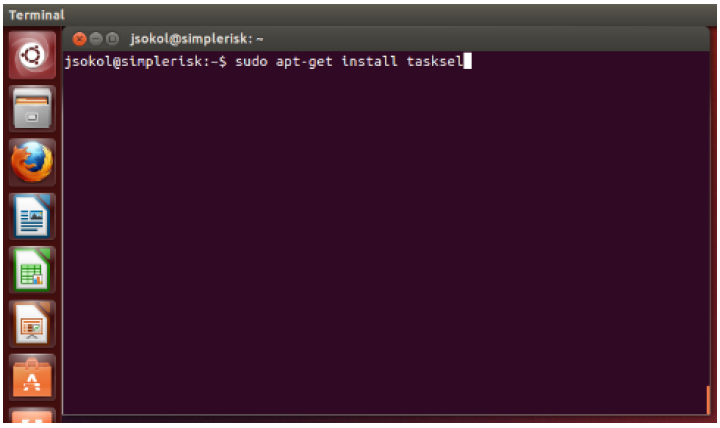


This will pull down the latest version information for all of the installed operating system files. Now run “sudo apt-get dist-upgrade” and answer “y” when it asks if you would like to continue.

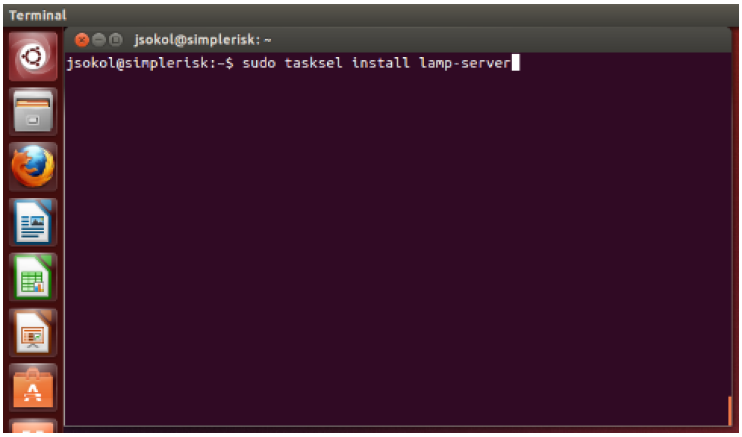


Installing Apache, PHP, and MySQL

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. You will know that this installation process is complete when the package configuration screen goes away and you are back at the terminal shell.

Next we will need to install a few extensions to ensure SimpleRisk will run properly using the following:

sudo apt-get install php-mbstring

sudo apt-get install php-ldap

We will also need the mcrypt module you will need to use the following commands to obtain install and setup mcrypt for PHP 7.2.

sudo apt-get install php-pear
sudo pecl channel-update pecl.php.net

sudo apt install php-dev libmcrypt-dev php-pear
sudo pecl install mcrypt-1.0.1 (when you see “sedlibmcrypt prefix? [autodetect] :” Just hit enter to continue)

You may need to adjust the following for your version of PHP (ex. etc/php/7.1/apache2/php.ini)

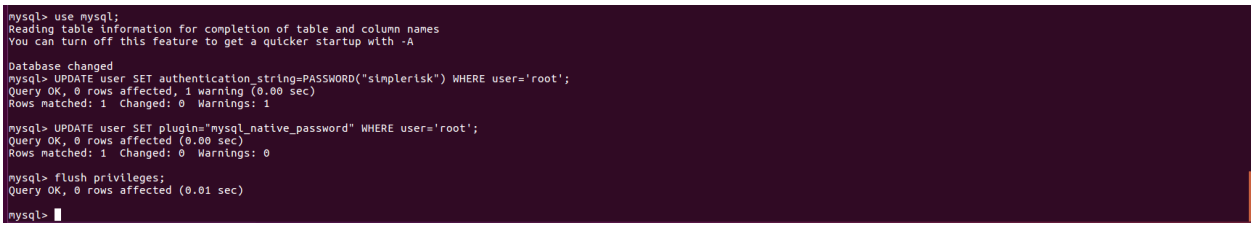
sed -i 's/;extension=xsl/;extension=xsl\nextension=mcrypt.so/g' /etc/php/7.2/apache2/php.ini
sed -i 's/;extension=xsl/;extension=xsl\nextension=mcrypt.so/g' /etc/php/7.2/cli/php.ini

Now we need to do a little setup of MySQL for the install to go smoothly, this will change the ROOT MySQL user password and you are welcome to change it again after the SimpleRisk database is installed.

First login to the MySQL console using "mysql -u root -p". The terminal will then ask for the password set in the MySQL installation setup.

Now in the console use the following to set the root password and confirm the plugin / change the plugin used for password authentication.

use mysql;
UPDATE user SET authentication_string=PASSWORD("simplerisk") WHERE user='root';
UPDATE user SET plugin="mysql_native_password" WHERE user='root';
flush privileges;



note: in this screenshot this has already been done hence 0 rows affected your should show 1 row affected.

The next step of setting up MySQL for a SimpleRisk install will be to set the sql-mode. To do this use the following steps:

1) use "vi /etc/mysql/mysql.conf.d/mysqld.cnf"

2) At the bottom of the config file add the following to set the sql-mode.

sql-mode="STRICT_TRANS_TABLES,NO_ENGINE_SUBSTITUTION"

```
#
# Error log - should be very few entries.
#
log_error = /var/log/mysql/error.log
#
# Here you can see queries with especially long duration
#log_slow_queries       = /var/log/mysql/mysql-slow.log
#long_query_time = 2
#log-queries-not-using-indexes
#
# The following can be used as easy to replay backup logs or for replication.
# note: if you are setting up a replication slave, see README.Debian about
#       other settings you may need to change.
#server-id              = 1
#log_bin                        = /var/log/mysql/mysql-bin.log
expire_logs_days        = 10
max_binlog_size   = 100M
#binlog_do_db           = include_database_name
#binlog_ignore_db       = include_database_name
#
# * InnoDB
#
# InnoDB is enabled by default with a 10MB datafile in /var/lib/mysql/.
# Read the manual for more InnoDB related options. There are many!
#
# * Security Features
#
# Read the manual, too, if you want chroot!
# chroot = /var/lib/mysql/
#
# For generating SSL certificates I recommend the OpenSSL GUI "tinyca".
#
# ssl-ca=/etc/mysql/cacert.pem
# ssl-cert=/etc/mysql/server-cert.pem
# ssl-key=/etc/mysql/server-key.pem
sql-mode="STRICT_TRANS_TABLES,NO_ENGINE_SUBSTITUTION"
```

3) Now write the file out (esc, :wq, enter).

Now we will configure Apache for the SimpleRisk API

1) Run the command “a2enmod rewrite” to enable mod_rewrite for Apache.

2) Open the file containing the Apache site configuration. This is likely found under

/etc/apache2/sites-enabled/000-default.conf.

3) Find the “Directory” section if it does not currently contain one add one for your SimpleRisk site match the contents to the screenshot so it looks like this::

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        <Directory "/var/www/html/simplerisk">
                AllowOverride all
                allow from all
                Options -Indexes
        </Directory>
        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

4) Restart Apache by running the command “service apache2 restart”.

Obtaining the SimpleRisk Files

Click on the FireFox logo in the Unity bar on the left. Once FireFox loads, enter https://www.simplerisk.com/ into the URL bar to go to the SimpleRisk site. Click on the “Download” link at the top.

Step 1

Choose Your Download Type: Install the SimpleRisk Web Files and Database Myself

Step 2

Download the Web Bundle: SIMPLERISK 20160612-001 WEB BUNDLE
Validate the Checksum: MD5 Checksum = 5a22619c0248a32985e3e8d45c21456f

Step 3

Download the Installer Script: SIMPLERISK 20160612-001 INSTALLER
Validate the Checksum: MD5 Checksum = 0a8881bd6ed29039988a3f3cc148f0fe

Step 4

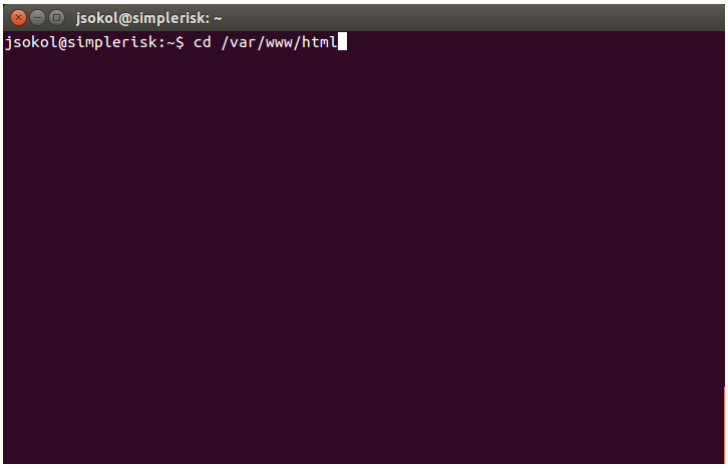
Follow the Instructions: INSTALL SIMPLERISK ON UBUNTU 13.04 (APACHE/MYSQL/PHP)

View All Releases and Release Notes

Click to download and save both the Web Bundle and the Installer Script. 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/html”.



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-20181103-001.tgz” (or whatever the most current version available is).

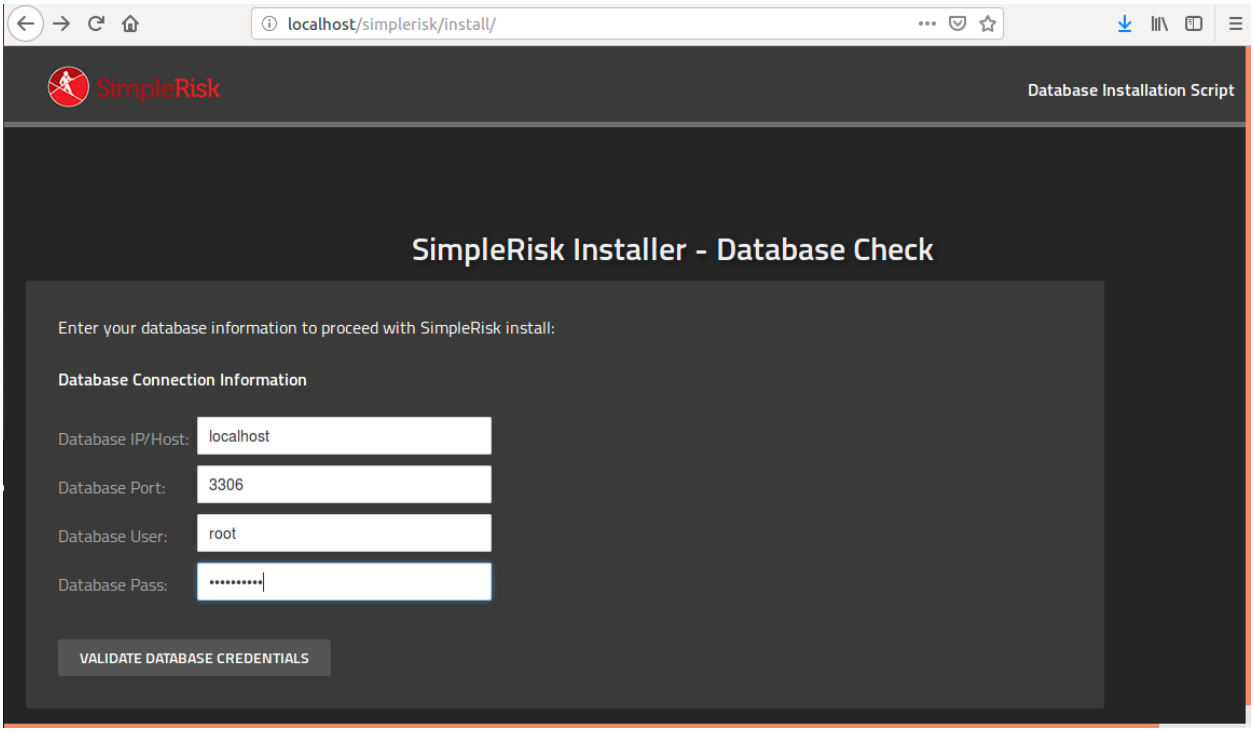
This will extract the files into a directory under the web root named “simplerisk”. You will need to access the files with a “/simplerisk” appended to the URL. Optionally, you can run the following commands to move it to the web root:

- sudo mv simplerisk/* .
- sudo rmdir simplerisk

Change the ownership permissions of the “simplerisk” directory and all its sub-directories to be owned by the www-data user (or whatever user Apache is running as) using the command “sudo chown –R www-data: /var/www/html/*”.

Installing the Database

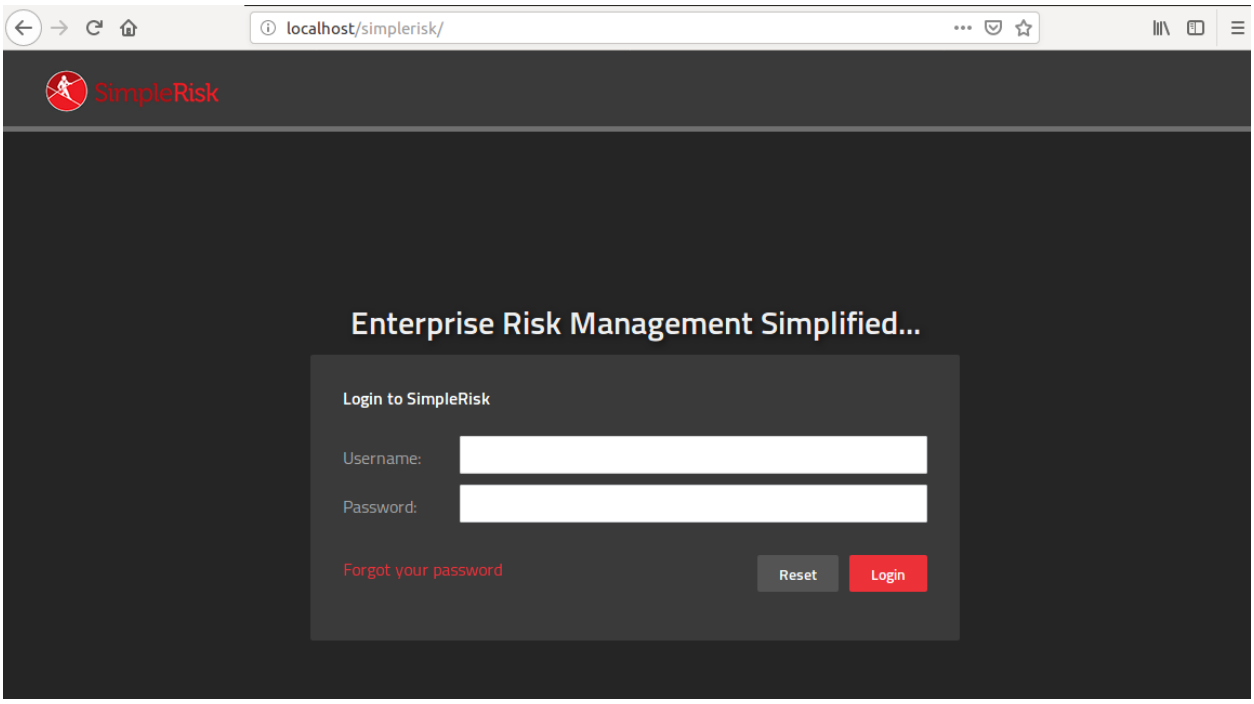
Extract the current SimpleRisk installer to the “simplerisk” directory using the command “sudo tar xvzf ~/Downloads/simplerisk-installer-20160612-001.tgz” (or whatever the most current version available is). This will create a new “install” directory. Next, in your web browser, navigate to http://localhost/install on your SimpleRisk instance. If everything works as expected, you will see an installer page designed to configure the database for you.



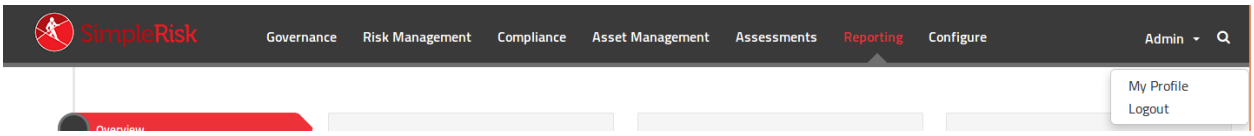
Under the Database Connection Information, provide it with your database hostname, port, username, and password (We set the root password to "simplerisk" in the previous step) Under the SimpleRisk Installation Information, provide it with the SimpleRisk database hostname, database name, and username that you would like SimpleRisk to use. A random password will be generated for the by default, it will generate a strong, randomly generated database password and we recommend that you keep that value. Under the SimpleRisk Configuration Information, you have the ability to choose the default language, session timeouts, default timezone, and other options. With the exception of the database schema language and timezone, we recommend that you keep the default values. When the script completes, it will ask if you would like to install a new /includes/config.php page. Select "Update" to have it automatically updated with the installer information. If it does not have permission to write to the file, or cannot find the existing config.php file, then it will provide you with the contents to place in it instead. It is always a good idea to delete the "install" directory once it is no longer needed using the command "sudo rm –r install".

Logging in to SimpleRisk

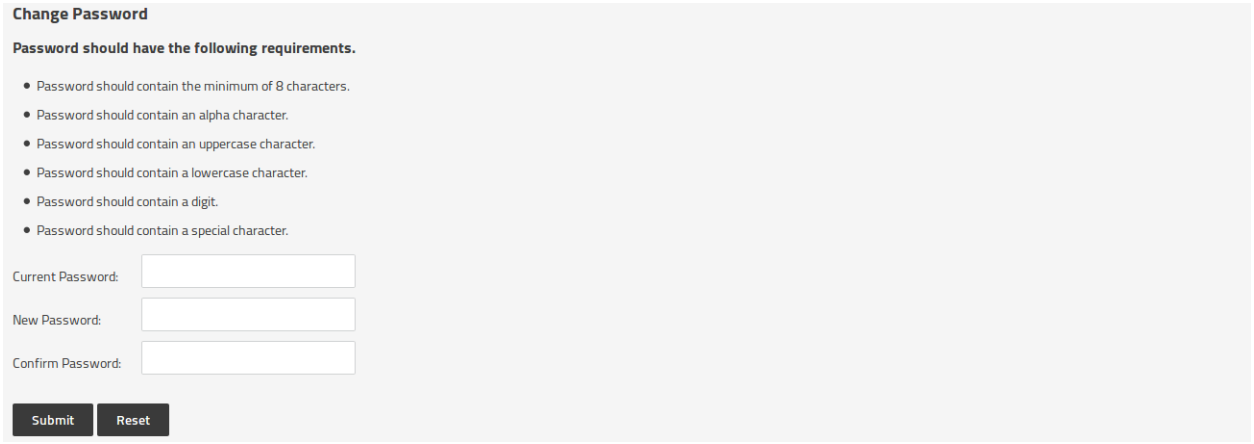
You should now have performed all of the steps you need to for SimpleRisk to be up and running. Now is the moment of truth where we hopefully get to see if all of your hard work paid off. You now need to point your web browser to the URL where SimpleRisk would be installed. If you followed the optional 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".



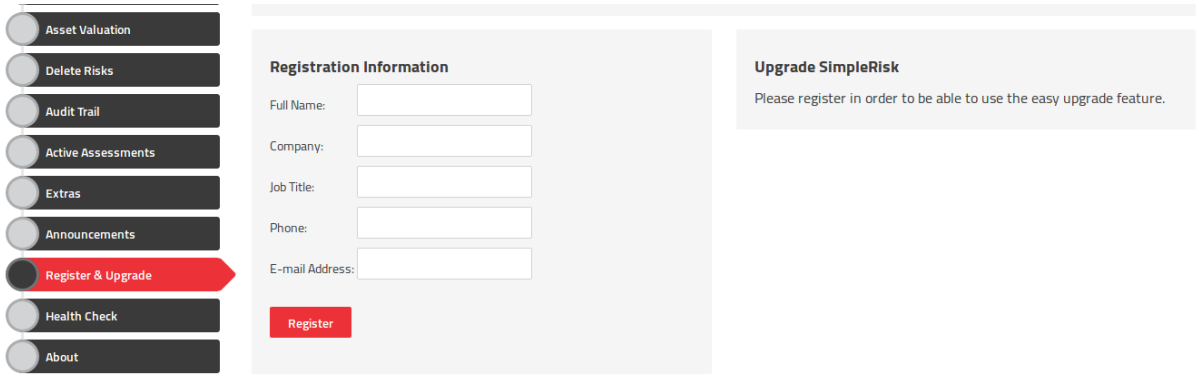
Enter your current password as “admin” and place a new long and randomly generated password into the “New Password” and “Confirm Password” fields. Then click “Submit”.



You should receive a message saying that your password was updated successfully. If so, then this is your new “admin” password for SimpleRisk. If you received a message saying that “The password entered does not adhere to the password policy”, you can change the policy by selecting “Configure” from the menu at the top followed by “User Management” on the left side. You will see a “Password Policy” section at the bottom of the page where you can change the policy and try changing your password again.

Registering SimpleRisk

This step is completely optional, but without it upgrades of SimpleRisk will require manual downloads of the new version, backing up your configuration file, extracting the new files, restoring the configuration file, and a database upgrade. It sounds like more effort than it really is, but we’ve made the process far simpler if you’re willing to tell us who you are. To register your SimpleRisk instance, select “Configure” from the menu at the top followed by “Register & Upgrade” from the menu at the left.



Enter your information and select the “Register” button. This will create a unique Instance ID for your SimpleRisk instance and download the Upgrade Extra which enables functionality for one-click backups and upgrades. If you run into issues with the registration process, we recommend that you check to ensure that the “simplerisk” directory and its sub-directories are writeable by the www-data user (or whatever user Apache is running as).

**** This completes your installation of SimpleRisk ****

SimpleRisk Paid Support and Extras

Everything that you’ve seen up to this point is completely free for you to install and use, forever. That said, we offer a number of ways for you to enhance your SimpleRisk instance with even more functionality. If you like what you see, and find it useful, please consider purchasing one of our inexpensive Paid Support plans or Extra functionality so that we can continue to offer you the best open source risk management tool available. Thank you!