INSTALLATION GUIDE

http://www.precurio.com

Klein Devort Ltd
29 Muili Street

Off Kudirat Abiola Way

Oregun, Lagos

NIGERIA

http://www.kleindevort.com

For Sales and Technical Support :

Tel: +234 1 7431704

Fax: +234 1 6281599

Online purchase: http://www.precurio.com/commercial-services.php

Support email:

support@precurio.com

This guide is frequently updated to reflect changes in the product. The latest version of this guide can always be found at

http://www.precurio.com/download/installation_guide_linux.pdf

This guide was prepared for Precurio Version 2.0.3 (May, 2010)

Table of Contents

Installing Precurio

Congratulations, you have just downloaded your copy of the Precurio Intranet Software. Precurio is very simple to use and you will probably not even need to read through this guide.

If you feel confident enough, simply take a look at the minimum system requirements and proceed to installing Openfire when you are finished installing precurio.

Minimum System Requirements

Any server on which you plan to install Precurio must have the following

Apache Server (version 2.2.11)

If you don't have one installed, then it is also likely you don't have other software (i.e. PHP and MySQL), required to run Precurio. You can easily get all of this software in one easy install package here.

Most of the modules needed by Precurio are enabled by default with the exception of these three(3) Your apache server must have the following modules loaded.

- o   mod_rewrite

- o   mod_proxy

- o   mod_proxy_http

To enable a certain module, simply locate your *httpd.conf* file in your apache installation, and edit accordingly.

Also make sure 'AllowOverride' is set to 'All' .i.e 'AllowOverride All' in your Directory configuration.

MySQL Server (version 5.x)

If you don't have one installed, you can easily get the free community edition server here. You can also get a free MySQL client here.

PHP Server (version 5.3.x)

You must have the following extensions enabled on your php server

- o   php_curl

- o   php_gd2

- o   php_ldap

- o   php_pdo_mysql

To enable a certain module, locate your *php.ini* file in your PHP installation, and edit accordingly.

Starting Installation

To start the installation, unzip the downloaded file and copy the precurio folder to your web root (i.e. the root directory of your web server, i.e Apache). Then point your browser to *"http://[YOURSERVERNAME]/precurio/public/install"* , for example *"http://kdl/precurio/public/install"*

If you get an error upon directing your browser to *"http://[YOURSERVERNAME]/precurio/public/install"*, please make sure you have met all the minimum requirements need to successfully install Precurio.

If you get an Internal Server Error, then it means you have not enabled mod_rewrite on your Apache server (Please see Minimum System Requirements). For other errors, please contact our support team at support@precurio.com.

Please note that the whole installation process is just a convinience method of editting the Precurio configuration file. In some unforseen situations, you may have to edit this file directly, you can find it at "/precurio/application/configs/precurio.ini"

General Settings

The screenshot above shows how to fill the general settings tab. Most fields are pretty self explanatory, but we shall explain some tricky ones.

Authentication Mechanism :

This enables you select how you want your users to be authenticated. You can either use the database, where you have to add each user , or connect to an already existing directory of your users, eg Microsoft Active Directory.

Email Domain
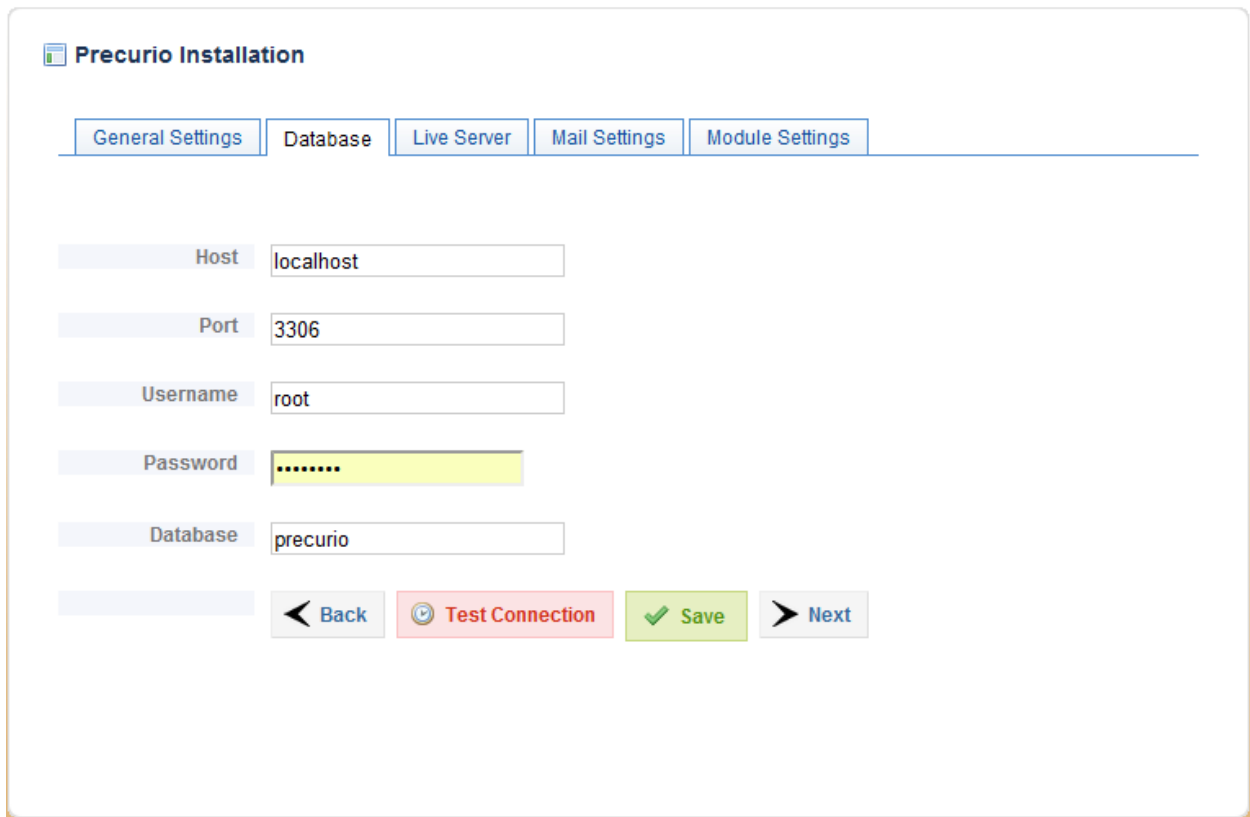
This is simply the "@xxxxxxx.xxx" part of your company's email address.

Domain

This is actually the account suffix of your directory service. An easy way to get this, is to copy the "@xxxxxxx.xxx" part of the mail property of any user in your active directory

This should be ignored if you are not connecting to a directory service like the Active Directory.

Setting up the Database

Host

The name or IP address of the computer on which you installed the MySQL server. If you installed on the same machine as the web server, simply leave it as '*localhost*'.

Port

The port number on which the MySQL server listens for connections. The default is 3306.

Username

The username you use to connect to your MySQL server. The default is "root"

Password

This is the password you use along with the username above. In a new MySQL installation, the password is blank.

Database

The name of the database Precurio should use. Though this can be changed to anything convinient for the administrator, we recommend you leave it as "precurio".

Integrating with Active Directory

Precurio can easily be integrated with any directory server, including OpenLDAP, all you need, is to have your directory settings with you. (*This step will be automatically skipped if you chose the database authentication mechanism in the* general settings)

The screenshot above shows an example of an active directory integration. You can always use the "*Test Connection*" button, to test if your settings are correct.

Always remember to click the "*Save*" button when you are done.

Setting up the live server

This page does not actually handle the live server setup process, as this involves a series of processes, properly explained in the installing Openfire section. That being said, on the part of Precurio, this is just where you need to configure.

Host

This is the name of the server on which you plan to install Openfire, which should typically be the same server on which you are installing Precurio (except you want to make things more complicated).

Service

This is the service Precurio is going to connect to. As of version 2.0.0, Precurio can only connect to the "/http-bind/" service.

Setting up the live server

Integrating with your Mail Server

Integrating with your mail server is a fairly technical process but can easily be done by the person who set-up your mail server. If you are not this person, please request your mail settings from your mail service providers.

Another way is to copy this settings from the "account settings" option of your current mail client.

Enabling and Disabling modules
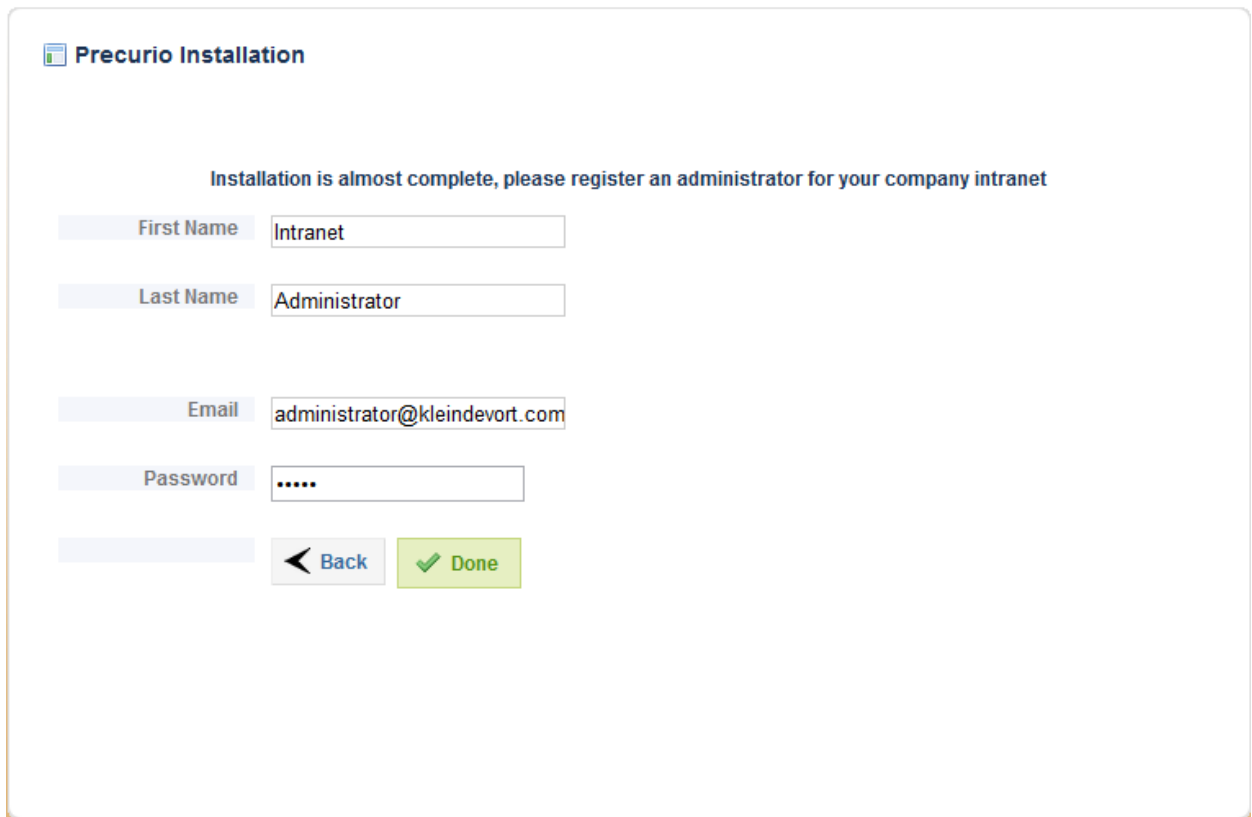
At this stage of the installation, you have the opportunity of not installing certain modules you don't want your users to access. Note that you can always enable this modules again anytime by going to "*admin->settings->modules*" from your web browser.

Creating your first user

Please note that, this step will automatically be skipped if you have chosen to authenticate through a directory service such as Microsft Active Directory.

After completing the previous steps, you will be asked to register an administrator for your company intranet. This administrator will be responsible for the initial setup of groups, roles and other users in the organisation.

Simply fill in your first name, last name, email and a password you can easily remember. Upon clicking the "Done" button, you will be taken to a login screen where you will be asked for a username and password.

Installing Openfire

Openfire is a powerful instant messaging (IM) and chat server from Jive Software, that implements the XMPP protocol. This document will guide you through installing Openfire.

Before proceeding, please make sure you have JDK or JRE 1.5.0 (i.e. Java 5) or later installed on your system. You can upgrade your Java installation by visiting *http://java.sun.com*.

Please note that you can always get settings you used during Precurio installation by logging in to Precurio, select the "admin" module, and select "settings" (i.e admin->settings).

Step 1

Click here to download Openfire.

Extract the Openfire folder to any location on your server (*it is recommend you copy it to "/opt/openfire/" or* "/usr/bin*").*

Throughout the rest of this guide, we are going to assume you copied the Openfire folder to the "opt" folder, hence the path to your Openfire installation is ASSUMED to be "/opt/openfire".

If you are opted to use the database authentication during Precurio Installation, the next step is very important, else if you chose LDAP Authentication, skip to step 3.

Step 2

If you are going to be using the database authentication, you have to integrate Openfire tightly with your Precurio database, to do that, open "/opt/openfire/conf/Openfire.xml".

The content of the file will look similar to this

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- root element, all properties must be under this element -->
<jive>
    <adminConsole>
        <!-- Disable either port by setting the value to -1 -->
        <port>9090</port>
        <securePort>9091</securePort>
    </adminConsole>

    <locale>en</locale>

</jive>
```

Now, between "<locale>en</locale>" and "</jive>" , you are going to paste the content below.

```
******************************* start here**************************************
<jdbcProvider>
    <driver>com.mysql.jdbc.Driver</driver>
    <connectionString>jdbc:mysql://localhost/precurio?user=root&amp;password=
    </connectionString>
  </jdbcProvider>
  <admin>
     <authorizedUsernames>admin,administrator</authorizedUsernames>
  </admin>
  <provider>
    <auth>
      <className>org.jivesoftware.openfire.auth.JDBCAuthProvider</className>
    </auth>
    <user>
      <className>org.jivesoftware.openfire.user.JDBCUserProvider</className>
    </user>
    <group>

<className>org.jivesoftware.openfire.group.JDBCGroupProvider</className>
    </group>
  </provider>
  <jdbcAuthProvider>
    <passwordSQL>SELECT password FROM user_details WHERE
username=?</passwordSQL>
    <passwordType>md5</passwordType>
  </jdbcAuthProvider>
  <jdbcUserProvider>
    <loadUserSQL>SELECT concat(first_name,' ',last_name) as full_name,email
FROM user_details WHERE username=?</loadUserSQL>
    <userCountSQL>SELECT COUNT(*) FROM user_details</userCountSQL>
    <allUsersSQL>SELECT username FROM user_details</allUsersSQL>
    <searchSQL>SELECT username FROM user_details WHERE</searchSQL>
    <usernameField>username</usernameField>
    <nameField>first_name</nameField>
    <emailField>email</emailField>
  </jdbcUserProvider>
  <jdbcGroupProvider>
    <groupCountSQL>SELECT count(*) FROM groups</groupCountSQL>
    <allGroupsSQL>SELECT title FROM groups</allGroupsSQL>
    <userGroupsSQL>SELECT title FROM user_groups join groups on
user_groups.group_id = groups.id WHERE user_id = (select user_id from
user_details where username = ?)</userGroupsSQL>
    <descriptionSQL>SELECT description FROM groups WHERE
title=?</descriptionSQL>
    <loadMembersSQL>SELECT username FROM user_groups join user_details on
user_groups.user_id = user_details.user_id WHERE group_id = (select id from
groups where title = ?)</loadMembersSQL>
    <loadAdminsSQL>SELECT username FROM user_groups join user_details on
user_groups.user_id = user_details.user_id WHERE group_id = (select id from
groups where title = ?)</loadAdminsSQL>
  </jdbcGroupProvider>
*******************************stop here**********************************
```

After pasting the content in the Openfire.xml file,

Please note line 4 (i.e. connectionString):

```
jdbc:mysql://localhost/precurio?user=root&amp;password=
```

This means we are connecting to a "Mysql" database named "precurio" located on "localhost" server, using username "root" and no password. Please change this to what you used in the database settings, during Precurio Installation

So, for example, you are going to have

```
jdbc:mysql://kdl/precurio?user=root&amp;password=ad214min
```

if you installed the MySQL server on the "kdl" server, and you connect using username "root"and password "ad214min" to the default Precurio database "precurio".

Also note line 8 (i.e admin):

```
<authorizedUsernames>admin,administrator</authorizedUsernames>
```

This means only admin and administrator will be allowed to login to the Openfire administrator console. If you used something other than admin@xxxxxxxxx.xxx or administrator@xxxxxxxxx.xxx when creating your first account, during Precurio installation, please include it in the comma seperated list.

So, for example, you are going to have

```
<authorizedUsernames>admin,administrator,smith</authorizedUsernames>
```

If, you used smith@xxxxxxxxx.xxx as your administrator's account, during Precurio installation.

Now save the Openfire.xml file, and proceed to step 3.

Step 3

To start Openfire, enter this in terminal "**./openfire start**" (make sure you are logged in as *root*).

You should get a reply "**Starting openfire**". Now launch your web browser and go to '**http://127.0.0.1:9090'** to begin the Openfire setup.

Step 4

Setting up Openfire is a relatively easy process. It begins with the *language selection*, then *Server Settings*, *Database Settings*, *Profile Settings* and finally *Admin Account*.

While setting up Openfire is pretty straighforward, there a few places we would like to offer our advice.

Server Settings : Domain

At the second step of the setup, you will be required to put in the host settings for your Openfire server, make sure the value you put in the "Domain" field corresponds to the same value you put in the "Host" field, when you were setting up the live server, during Precurio Installation.

Database Settings

When asked to choose between a "Standard Database Connection" or "Embedded Database", choose the "Standard Database Connection".

Database Settings : Database URL

The host name is the name of the computer you installed the MySQL server, if it is the same computer as the one on which you are installing Openfire, put in "localhost".

The database name is the name of the database to use for Openfire, use the same database you used when setting up your database during Precurio installation.

So your database URL should look something similar to this :

jdbc:mysql://localhost:3306/precurio

Profile Settings

Choose "Default", if you are using the database authentication mechanism for Precurio, else choose "Directory Server".

Admin Account

Click the "Skip this Step " button if you selected the database authentication mechanism during Precurio Installation, else add as many administrators as you want, then click "Continue".

Step 5

IMPORTANT : If you are authentication through a directory server such as Active Directory or OpenLDAP, please skip this step and proceed to step 6.

Just after finishing the Openfire installation, right before you login to the Openfire Administrator console. Open up your browser and enter a url similar to this;

"http://kdl/precurio/public/chat/index/integrate " (note "kdl" is the name of my web server, use yours.)

You should see a page telling your Openfire has been successfully integrated with Precurio, as shown below.
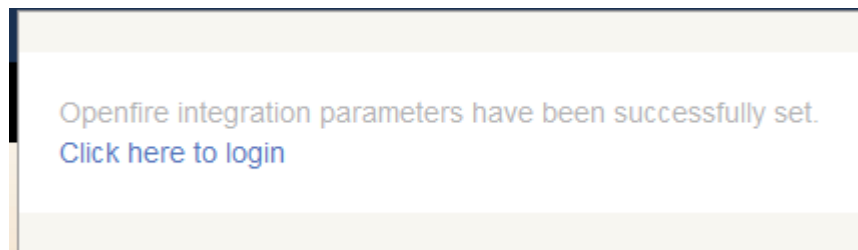
Step 6

- Stop and Start the Openfire program
- Login to the Openfire administrator console
- Select the "Plugins" tab

- Select "Avaliable Plugins"
- If you can't find the "Broadcast" plugins on the list of available plugins, scroll down and click the "Update Now" link, to update the list.
- Now click the plus "+" sign, to install the "Broadcast" plugin.
- Stop and Start the Openfire program.

Step 7

This step is actually the most problematic because even though what you want to achieve is relatively simple, sometimes for some weird reasons, it might not just work.

What we want to do, is to let your Apache server be aware of your Openfire server. And the only way to do this, is to forward all '/http-bind/' requests coming to your web server (Apache) to 'http://[YOUR-DOMAIN]:7070/http-bind/', i.e Openfire.

To do this, open your Apache "httpd.conf" file and put in the configuration below

```
ProxyRequests off

ProxyPass /http-bind/ http://[YOUR-DOMAIN]:7070/http-bind/
```

Save the "httpd.conf" file. Before restarting your Apache server, point your web browser to this url ; "http:// [YOUR-DOMAIN]/http-bind/", your brower should display a "page not found" error.

Now restart Apache, and point your web browser to the same url, this time you should either get a 'bad url' error, or a 'forbidden access' error. (*If your apache does not restart successfully, make sure you 'mod-proxy' and 'mod-proxy-http' enabled. see minimum requirments*)

If you get a 'bad url' error, congratulations, please proceed to step 8. If you get a 'forbidden access' error, open your Apache "httpd.conf" file again and put in this configuration

```
<proxy>

Order deny, allow

Allow from all

</proxy>
```

(Please make sure there is no other `proxy` tag, else do not add this one, edit the already existing one.)

Save the "httpd.conf" file and restart Apache, you should now get a 'bad-url' error if you refresh your browser.

IMPORTANT!!! If you are using a virtual host setup, all this configurations MUST be put in between the opening and closing `VirtualHost` tags.

Step 8 (Final Step)

You have finally set up openfire, and have installed the "Broadcast" plugin. Everything thing should be working fine now (one way to know, is to login to Precurio and the Chat status will no longer be "Disconnected"), but there is one problem, you will always have to start the Openfire program each time the systems starts.

If you would like to install Openfire as a service, two scripts are provided in the **bin/extra** directory:

- redhat-postinstall.sh -- automatically installs Openfire as a service on Red Hat. It does so by creating a "jive" user and then copying the openfired script to your init.d directory. This script must be run as root. Please see the comments in the script for additional information.

- openfired -- script to run Openfire as a service. You must manually configure this script. See the comments in the script for additional details.

Congratulations you have just completed installing Precurio and integrating with Openfire. If you had any problems with the installation, please visit our forums *here*, or create a new support request *here*.

NOTE : if you purchased the PRO version, you contact our experienced technical team at support@precurio.com.

Getting Started with Precurio

After installling Precurio and integrating with Openfire, there are a few things you should do before giving your users access to the intranet. This section discusses them in details;

Setting up Precurio Daemon

Precurio has a daemon script, "/precurio/bin/daemon.php" , which needs to be run at intervals (30 mins), this script helps Precurio in the proper management of your intranet, and handles tasks such as, email notifications, RSS feeds fetching etc.

To make this script run frequently, you will need to make it a cron job.

Creating Groups

Groups in Precurio are used in categorizing users, this categorisatiion could be in form of roles, departments or locations. One of the first things you should do after installing Precurio is to creating various groups, especially role groups.

You can create groups by going to the "Admin" module, select "Groups", and click the "Add" Button. When adding a group you can choose to indicate if the group is a Department, Role or Location. Note that a group may serve more than one categorisation purpose, i.e. a group could be both a Department and a Role.

After creating groups you should immediately begin adding members i.e. users.

Creating Access Rules

You don't want every user on your network to have access to the entire intranet, you want to limit each user's access to different parts of the intranet, and the way to do this is by creating access rules.

Access rules can only be created on roles, so to create an access rule, go to the "Admin" module, select "Roles" and click on "View" to configure the access rules for a particular role.

Administrator Tools - Roles - Role Details   Back | Forward

Roles

Title	Administrators
Description	IT administrators only
Parent Group	staff

Access Rules

	add	view	delete	edit	details	share	export	import	
Admin	●	●	●	●	●	●	●	●	Edit
Content	●	●	●	●	●	●	●	●	Edit
Chat	●	●	●	●	●	●	●	●	Edit
Contacts	●	●	●	●	●	●	●	●	Edit
Core Application	●	●	●	●	●	●	●	●	Edit
Staff Directory	●	●	●	●	●	●	●	●	Edit
Events	●	●	●	●	●	●	●	●	Edit
News	●	●	●	●	●	●	●	●	Edit
Polls	●	●	●	●	●	●	●	●	Edit
Task	●	●	●	●	●	●	●	●	Edit
Personal Page	●	●	●	●	●	●	●	●	Edit
Profile Page	●	●	●	●	●	●	●	●	Edit
Workflow	●	●	●	●	●	●	●	●	Edit

Group Members

If you are doing this for the first time, It is very important you first create access rules on the role you belong to, else you and your users will not be able to access the intranet anymore. i.e you will probably belong to role group called "Administrators", make sure your access rules allows that role access to every part of the intranet.