# How to install Openfire Meetings on ClearOS

2021-07-20: WikiSuite will now support all major Linux distros. Thus, the information below is no longer updated. It may still be valid, or not. It will be eventually removed from this site, so anything relevant should be moved to the appropriate site. For anything related to ClearOS, please search among the following: ClearOS site, code base, Developer docs, Wiki or forum.

Please contact us if you would like to help out.

Openfire is a real time collaboration (RTC) server supporting XMPP (Jabber) and WebRTC. See also Why Openfire.

# Quick upgrade

**2018-04-23 New versions Openfire 4.2.3 / app-openfire 1.2.8**

**How to install**

```
yum --enablerepo=clearos-contribs-testing install app-openfire
```

**How to upgrade**

```
yum --enablerepo=clearos-contribs-testing upgrade openfire app-openfire
```

# Quick install

Openfire can be installed with the following command on a ClearOS 7.4 box:

1)

```
yum --enablerepo=clearos-contribs-testing install app-openfire
```

2) Go to "System / Accounts / Users" in the menu to:
- Create some users (make sure the "Openfire User" is enabled in App policies for the user you create).

3) Go to "Server / Communication and Collaboration / Openfire" in the menu to:
- Click "Install and Initialize Built-in Directory". (Grab a coffee, this will take several minutes.)
- Click "Configure security Certificates" (TODO: Document what happens when Lets encrypt is enabled : http://wikisuite.org/How-to-install-Let-s-Encrypt-SSL-certificates-on-ClearOS).
- Select the admin user.
- Set the XMPP domain.
- Set the Openfire hostname from one of the available SSL certificates on the system. It is HIGHLY

recommended that you use LetsEncrypt for this.

4) Follow the link and log in to Openfire.

ClearOS integration includes:
- ClearOS Openfire app
- Openfire
- Plugins: Fastpath, Openfire meetings, Monitoring
- System database provisioning
- LDAP integration
- focus user (openfire-focus) for Openfire meetings
- Letsencrypt

# Detailed Install

## Assumptions

- This guide assumes your ClearOS server will be the main server for your domain. Thus, your website (powered by Tiki, which includes the ConverseJS XMPP client) will be on the same server.
- You can create e-mails accounts for your domain. This can easily be handled by ClearOS or by your domain name provider.

## Information

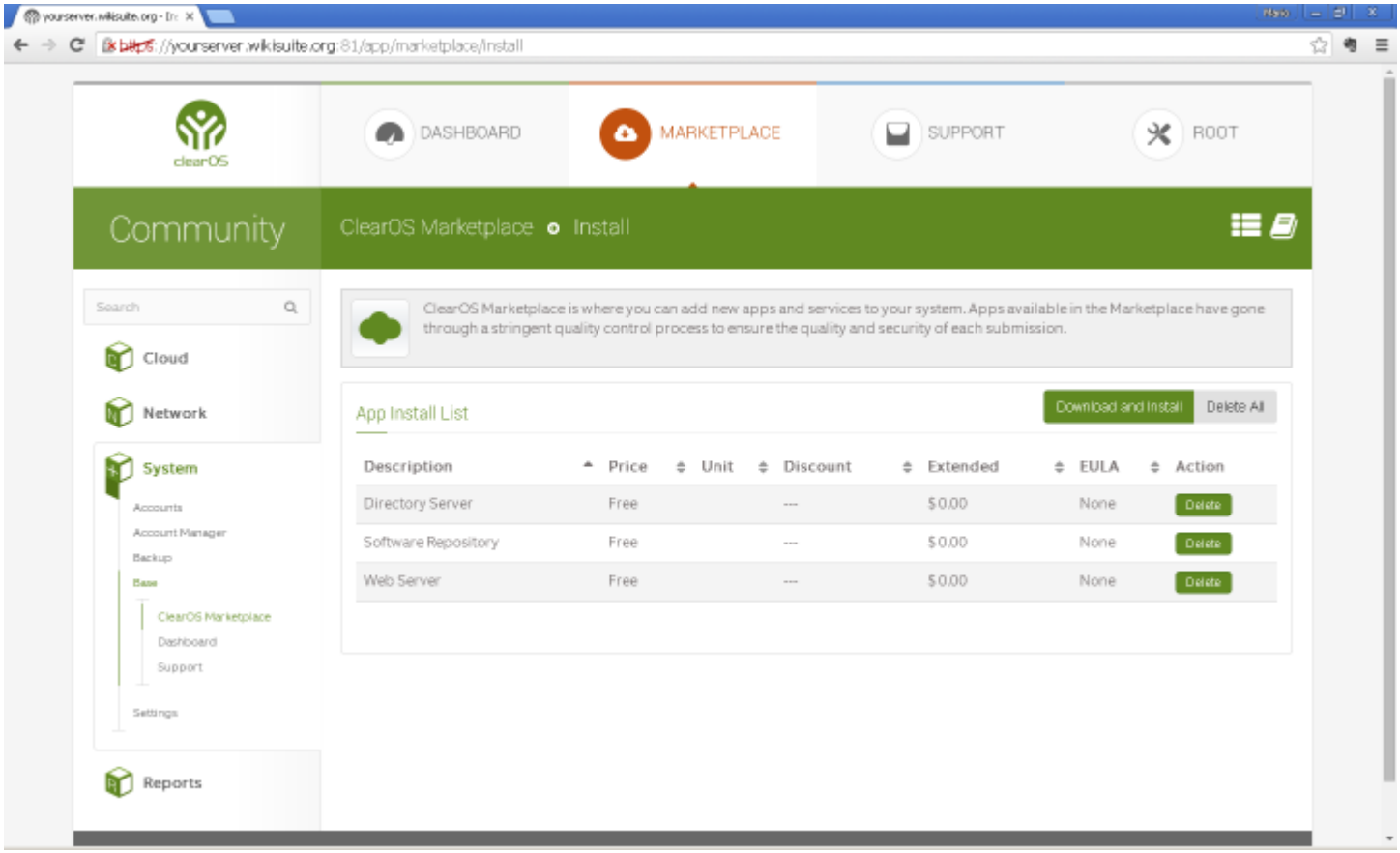
To Install Openfire 4.x on ClearOS 7.x within the WikiSuite environment follow these steps:

1.- Install a fresh ClearOS Server; be sure to run the latest Software updates to the core system.

2.- Make sure the clearos-epel repository is enabled

3- Include in the installation of:

a. The Web Server




# Configure domain name

How to set domain name on ClearOS

> Please note that Openfire is not multi-tenant, so it is designed to handle just one domain name. Ref: OF-162

# Install Openfire

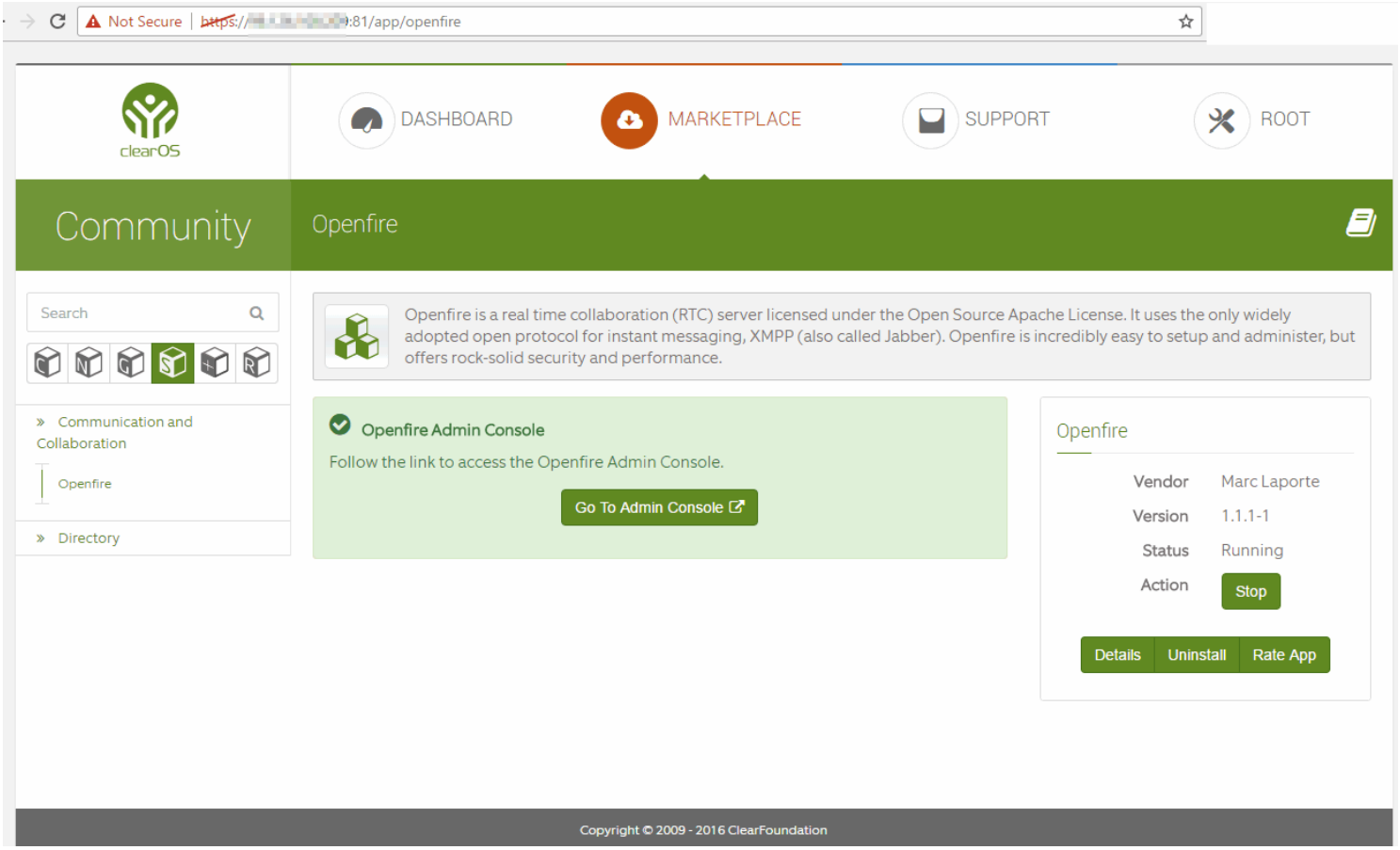
1.-Log in to your ClearOS via SSH using root.

2.-Install the Openfire app.

Type:

```
yum --enablerepo=clearos-contribs-testing install app-openfire
```

Go to "Server / Communication and Collaboration / Openfire' in the menu (https://yourserver.wikisuite.org:81/app/openfire):




# Configure OpenLDAP

1.-Click "Install and Initialize Built-in Directory". (Grab a coffee, this will take several minutes.)
1.-Initialize your OpenLDAP service through the Webconfig-Open LDAP Directory Server Module (https://yourserver.wikisuite.org:81/app/openldap_directory).

File not found.

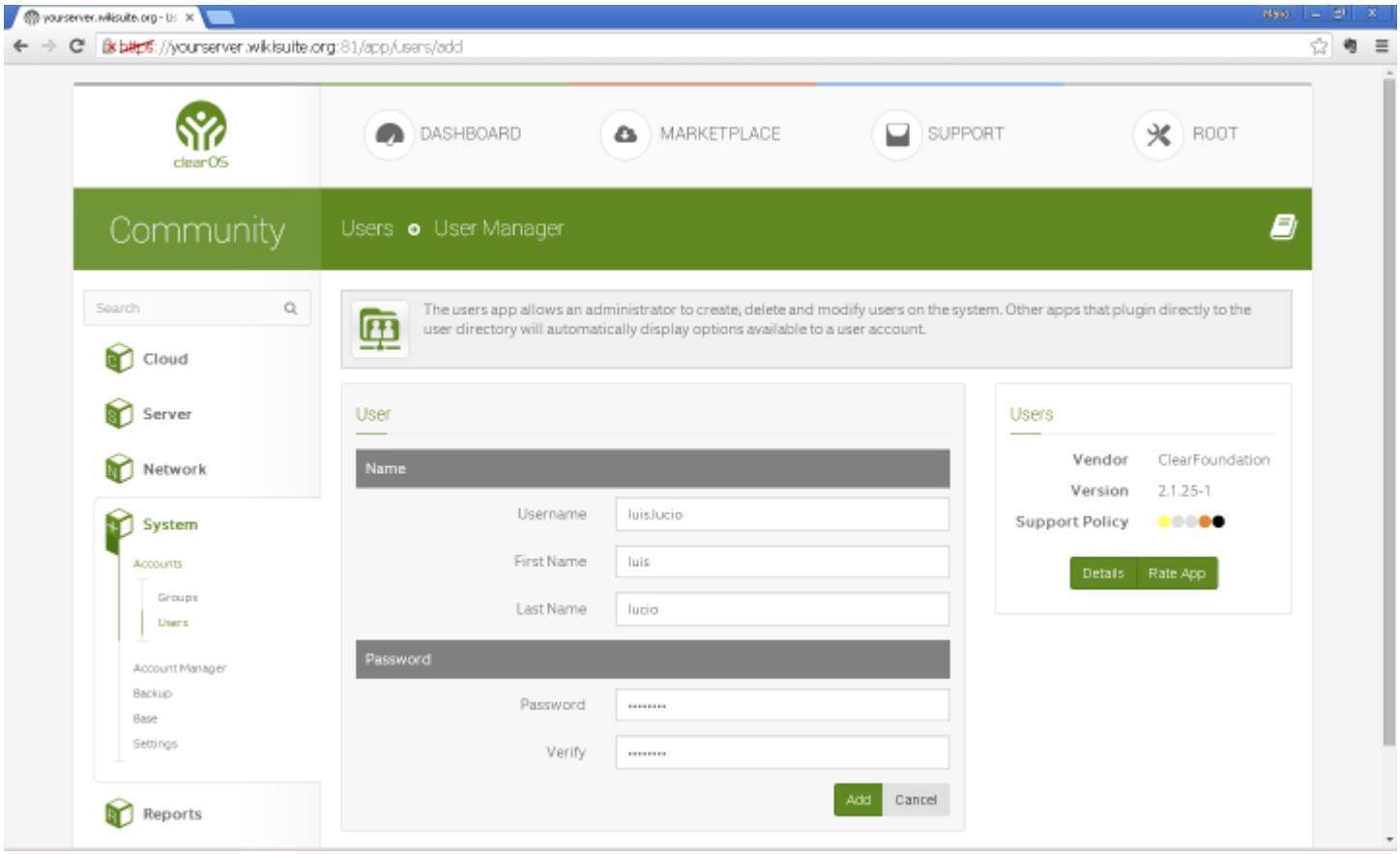
2.-On the Directory Server Settings page, set the server mode and Base Domain (https://yourserver.wikisuite.org:81/app/openldap_directory/settings/edit).

File not found.

3.-On the Directory Server Policies page, set the Publish Policy and Accounts access according to your requirements (https://yourserver.wikisuite.org:81/app/openldap_directory/policies/edit).

File not found.

4.-Don't forget to create one or two users as they will be used in the Openfire configuration phase. Use: (https://yourserver.wikisuite.org:81/app/users/add).




# Configure SSL certificates / Let's Encrypt

- We highly recommend you use Let's Encrypt. Especially since as of this writing (2018-04-01, no joke...), self-signed certificate integration isn't fully functional (see https://github.com/WikiSuite/app-openfire/issues/7).
  - If you want to use it, make sure LetsEncrypt is fully set up before you continue (See http://wikisuite.org/How-to-install-Let-s-Encrypt-SSL-certificates-on-ClearOS).

Go to "Server / Communication and Collaboration / Openfire" in the menu (https://yourserver.wikisuite.org:81/app/openfire):

1. Click "Edit" in "Setting"
2. Select the security certificate you want to use.

**Important notes:**

- As ClearOS also manages SSL certificates, they can co-exist independently as their storage files are different and independent. That is, Openfire generated certificates will only be used within Openfire applications.
- As of this writing (2018-04-01, no joke...), Directory Watcher (hot-deploy,

https://yourserver.wikisuite.org:9091/plugins/certificatemanager/certificate-management.jsp ) isn't integrated into the ClearOS app (see https://github.com/WikiSuite/openfire/issues/5). Upon Let's Encrypt certificate expiration, just re-do the setup step above, not changing your certificate selection and your certificate will be updated.

- You can access the OpenFire certificate store at: https://yourserver.wikisuite.org:9091/security-certificate-store-management.jsp

# Configure Firewall

The Openfire app will take care of opening the following ports:

| Port | TCP/UDP | Access Control | Application | Description |
|---|---|---|---|---|
| 5222 | TCP | Public | Openfire | The standard port for clients to connect to the server. Offers encryption via StartTLS |
| 5223 | TCP | Public | Openfire | Direct SSL/TLS port for clients to connect to the server. |
| 7443 | TCP | Public | Openfire | The port used for secured HTTP client connections. |
| 9091 | TCP | Administrative | Openfire | The port used for secured (HTTPS) Admin Console access. |

However, you will probably want to open more than those. ClearOS's Firewall should configured to block all ports, and open the following:

| Port | TCP/UDP | Access Control | Application | Description |
|---|---|---|---|---|
| 22 | TPC | Administrative | SSH | Terminal access |
| 25 | TCP | Public | OFMeet | SMTP: For emails for Openfire Meeting Planner |
| 80 | TCP | Public | (generic) | Web server (HTTP) |
| 81 | TCP | Administrative | ClearOS | Webconfig |
| 143 | TCP | Public | OFMeet | IMAP: For emails for Openfire Meeting Planner |
| 443 | TCP | Public | (generic) | Web server (HTTPS) |
| 587 | TCP | Public | OFMeet | SMTP For emails for Openfire Meeting Planner if you use Gmail |
| 993 | TCP | Public | OFMeet | IMAPS For emails for Openfire Meeting Planner |
| 4443 | TCP | Public | OFMeet | RTP over TCP for Jitsi Videobridge (fallback media proxy for video conferencing) |
| 5222 | TCP | Public | Openfire | The standard port for clients to connect to the server. On this port plain-text connections are established, which, depending on configurable security settings, can (or must) be upgraded to encrypted connections. |

| | | | | |
|---|---|---|---|---|
| 5223 | TCP | Public | Openfire | The port used for clients to connect to the server using the direct SSL/TLS method. Connections established on this port are established using a pre-encrypted connection. This type of connectivity is commonly referred to as the "old-style" or "legacy" method of establishing encrypted connections., but is not inherently 'less' secure. Configuration details can be modified in the security settings. |
| 5269 | TCP | Public | Openfire | The port used for remote servers to connect to this server. Connections established on this port are established using a pre-encrypted connection. This type of connectivity is commonly referred to as the "old-style" or "legacy" method of establishing encrypted connections. Configuration details can be modified in the security settings. |
| 7070 | TCP | Public | Openfire | The port used for unsecured HTTP client connections. |
| 7443 | TCP | Public | Openfire | The port used for secured HTTP client connections. |
| 9090 | TCP | Administrative | Openfire | The port used for unsecured (HTTP) Admin Console access. |
| 9091 | TCP | Administrative | Openfire | The port used for secured (HTTPS) Admin Console access. |
| 10000 | UDP | Public | OFMeet | Single UDP port multiplexing of multiple media streams (preferred media proxy for video conferencing) |
| 50000-60000 | UDP | Public | OFMeet | Dynamically allocated ports for media streams (fallback media proxy for video conferencing) |

Notes:

- Ports 7070 and 9090 are used for plain HTTP traffic. Each have a more secure HTTPS counterpart: 7443 and 9091 respectively. Consider disabling the HTTP ports, which could hurt interoperability and performance, but will increase security.

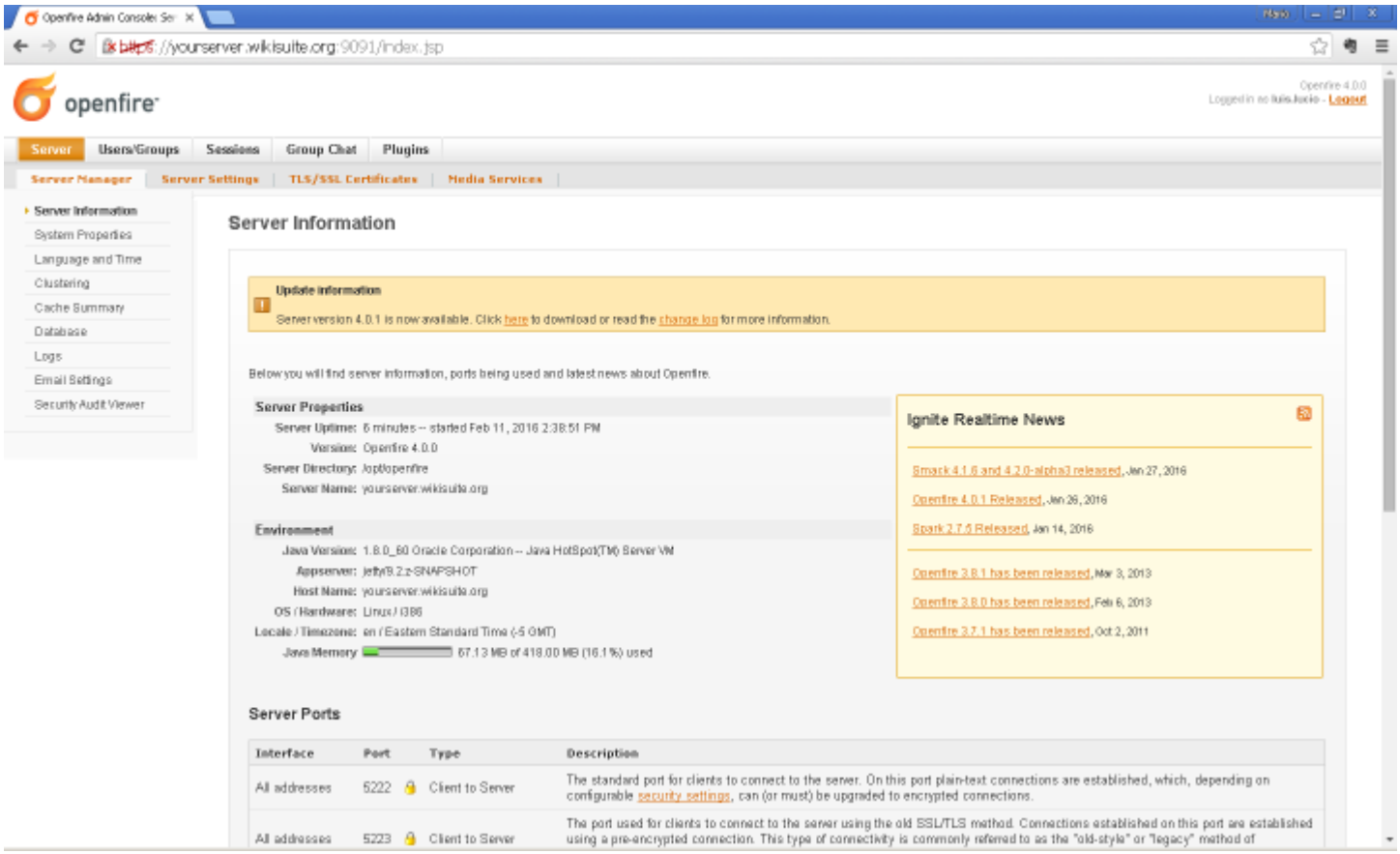
# Configure Openfire

**WARNING**: 2018-03-12: In openfire 4.2.2, plugins don't upgrade properly: apparently fixed in 4.2.3 (https://issues.igniterealtime.org/browse/OF-1464), which isn't released as of this writing.

1.- Use a web browser to connect to the admin console. The default port for the web-based initial setup admin console is 9090 (9091 for https). Initial setup and administration can be done from a remote computer using LAN IP address instead or hostname if it is resolvable by the remote computer, i.e. (https://yourserver.wikisuite.org:9090). The link is provided in the Openfire app for ClearOS.

WikiSuite: The most comprehensive and integrated Open Source enterprise solution.

Source: http://www.igniterealtime.org/builds/openfire/docs/latest/documentation/install-guide.html




# Install and configure Openfire Plugins

The Openfire app for Clearos will have already installed and done basic setup of the following plugins:

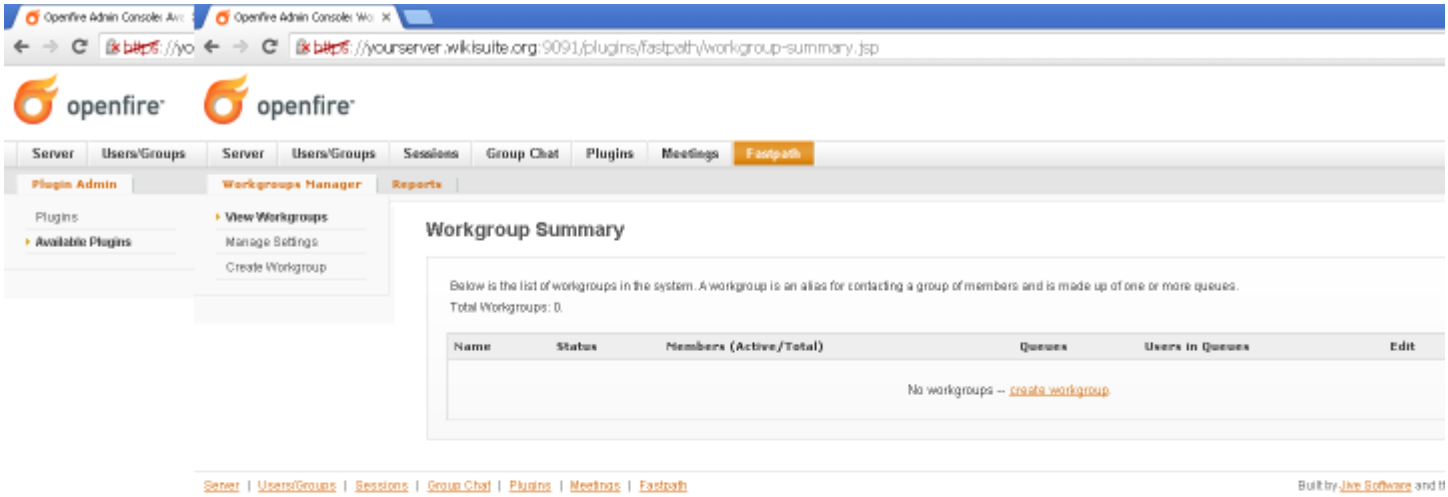
- Openfire Meetings Plugin (For group video conference)
- Openfire Fastpath plugin (For support chat: http://wikisuite.org/Fastpath)
- Monitoring plugin (for Message Archive Management support)

## Configure Openfire Meetings Plugin

1.- For security, Openfire Meetings Plugin creates a user named "focus". The openfire-app will create this user in ClearOS for you.

## Configure Openfire Fastpath plugin

1.- Once the plugin has been successfully installed, the Fastpath tab should be available, click on it to configure Workgroups (https://yourserver.wikisuite.org:9091/plugins/fastpath/workgroup-summary.jsp).



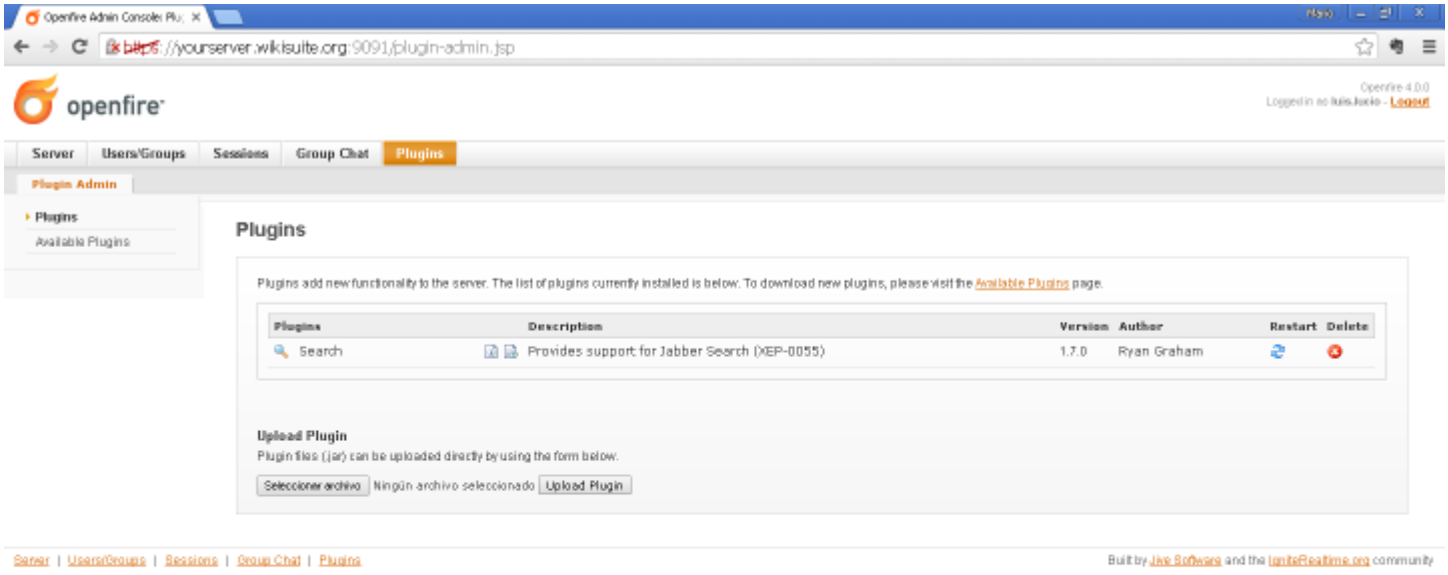

Notes:

- You can find a Quick start guide here: http://wikisuite.org/Fastpath.
- The snippet is provided on the Openfire Admin Console (Fastpath -> Workgroup Manager -> Workgroup Settings -> Text).
- jivelive.jsp is available on https://example.org:9091/webchat/jivelive.jsp - perhaps you'll need to edit the snippet above, if you're redirecting access to that resource through a reversed proxy.
- There's a simple landing page here: https://example.org:9091/webchat/ .

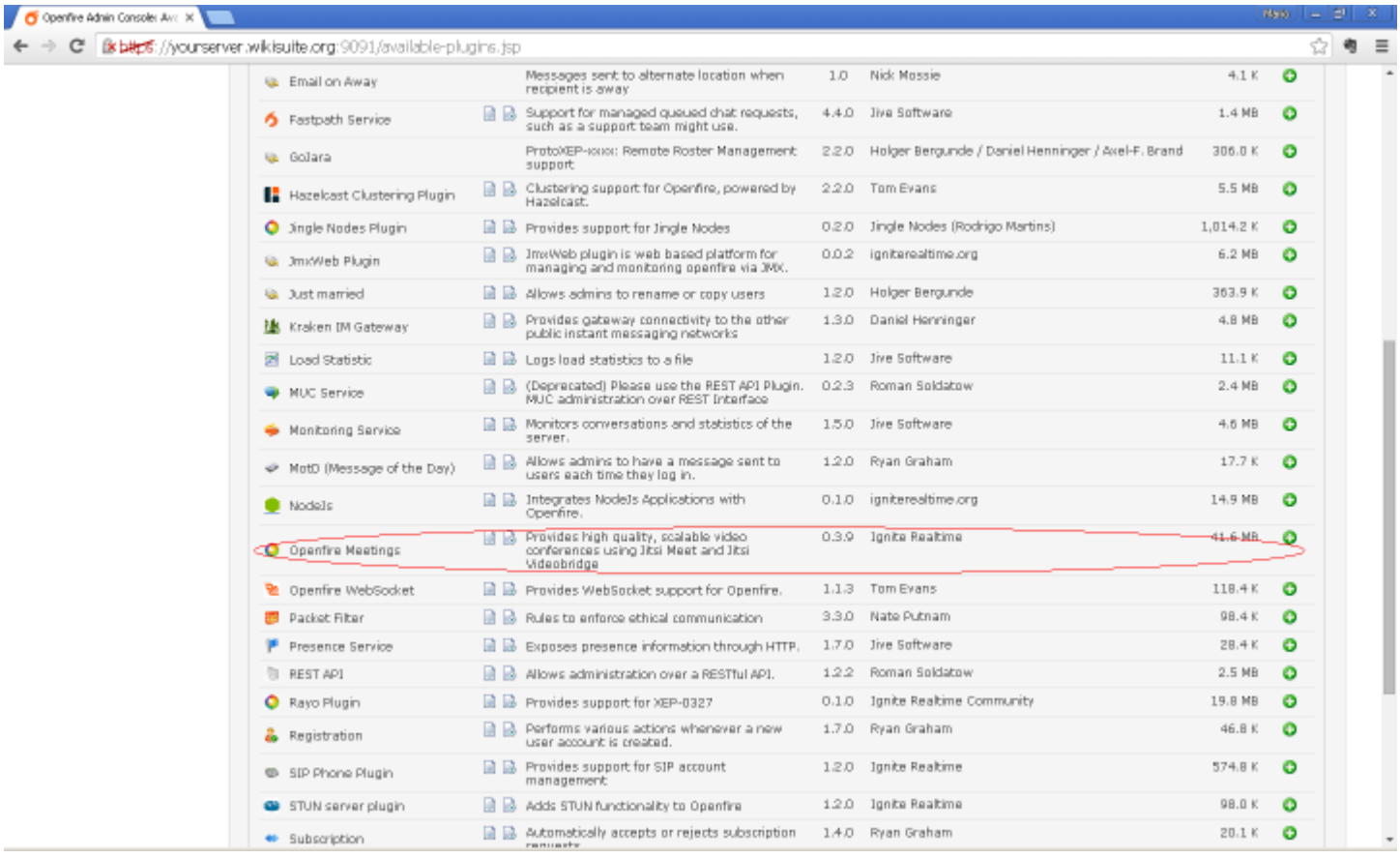
## Install additional Openfire plugins

1.- Log in to your Openfire Admin Console with an administrator user.

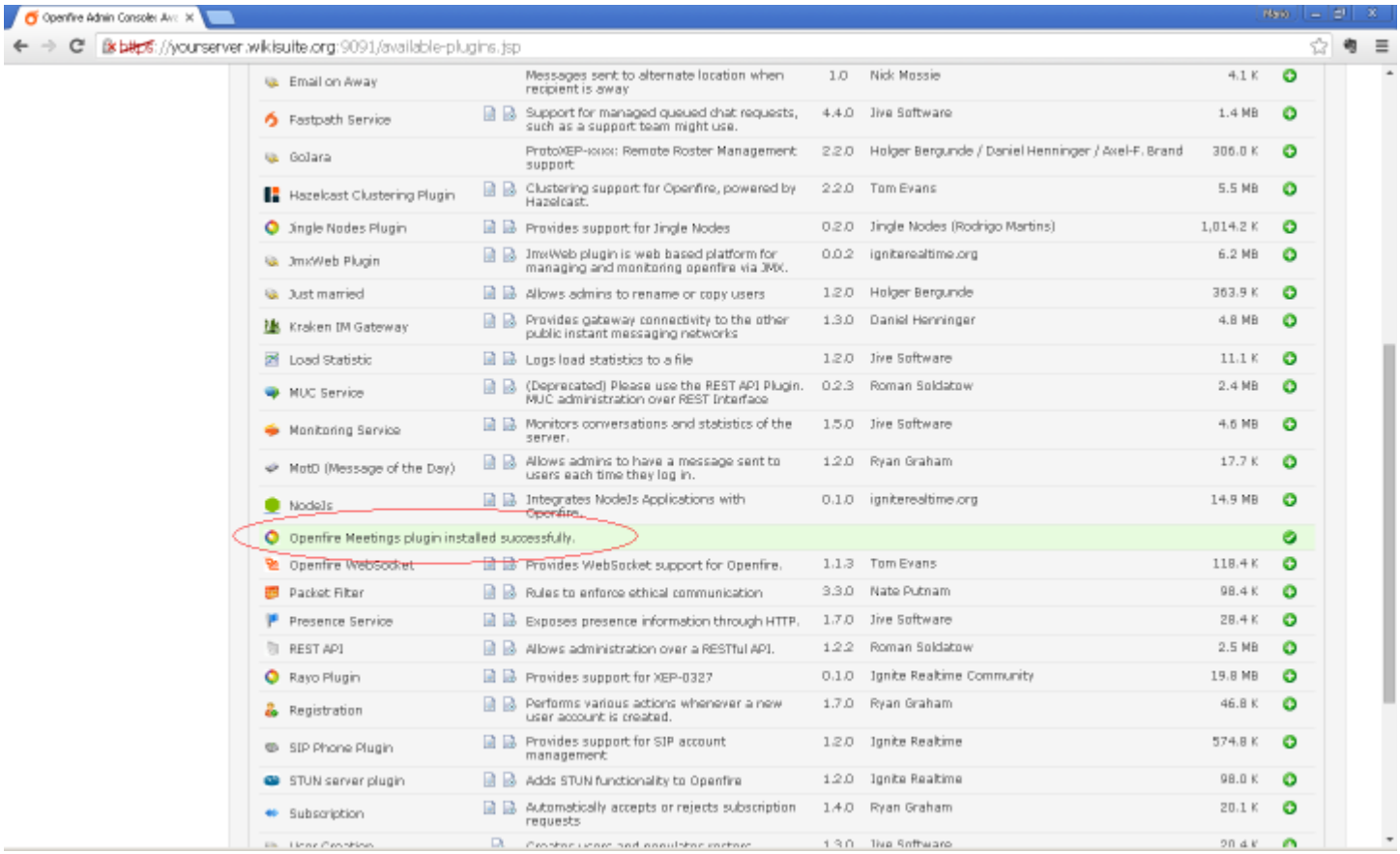
2.- Click on the Plugins Tab to manage Plugins




3.- Click on the available plugins link and scroll down to find the plugin you want.



4.- Click on then ¨+¨ to add the plugin to the Openfire server.

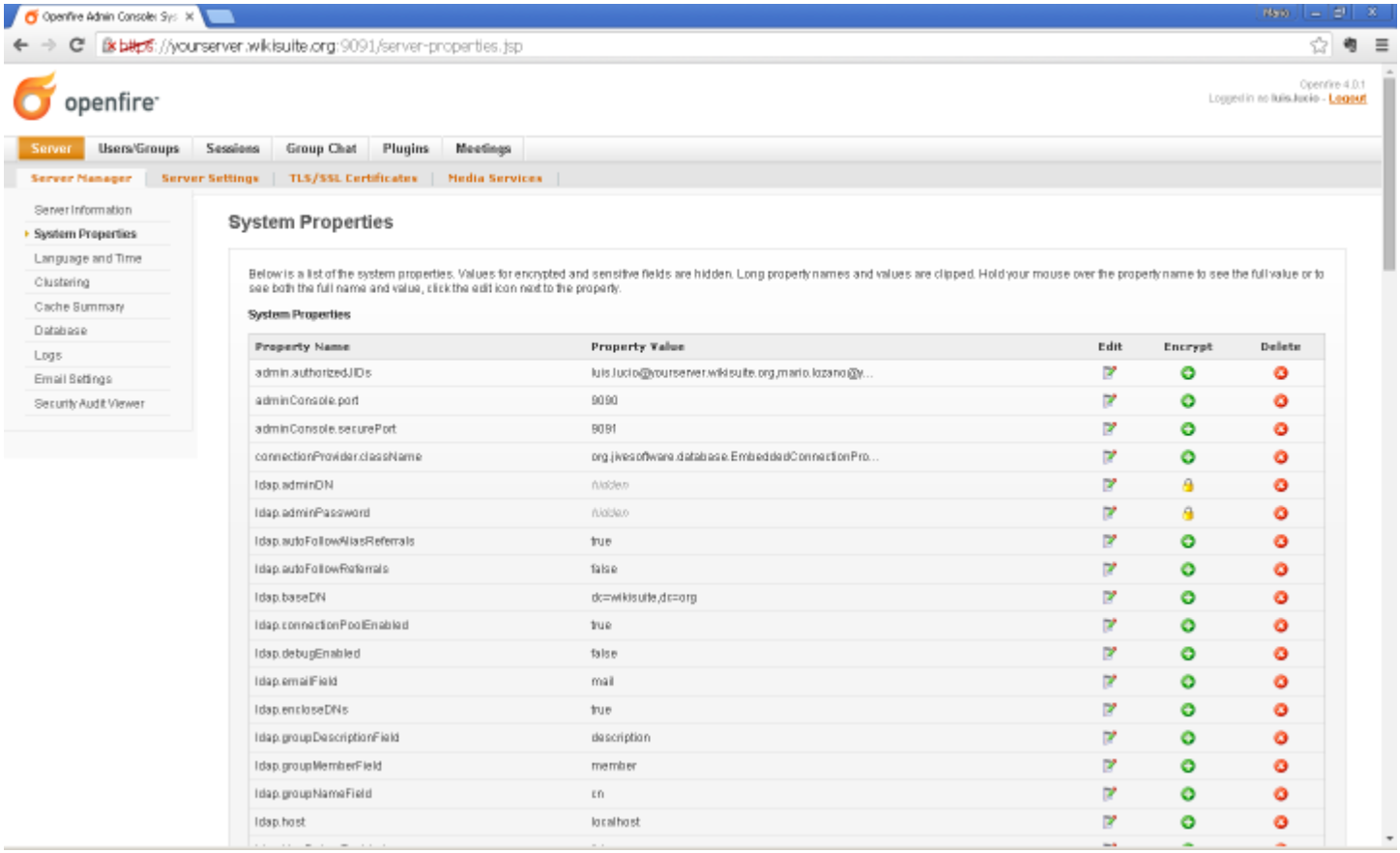



## Add more Openfire admins

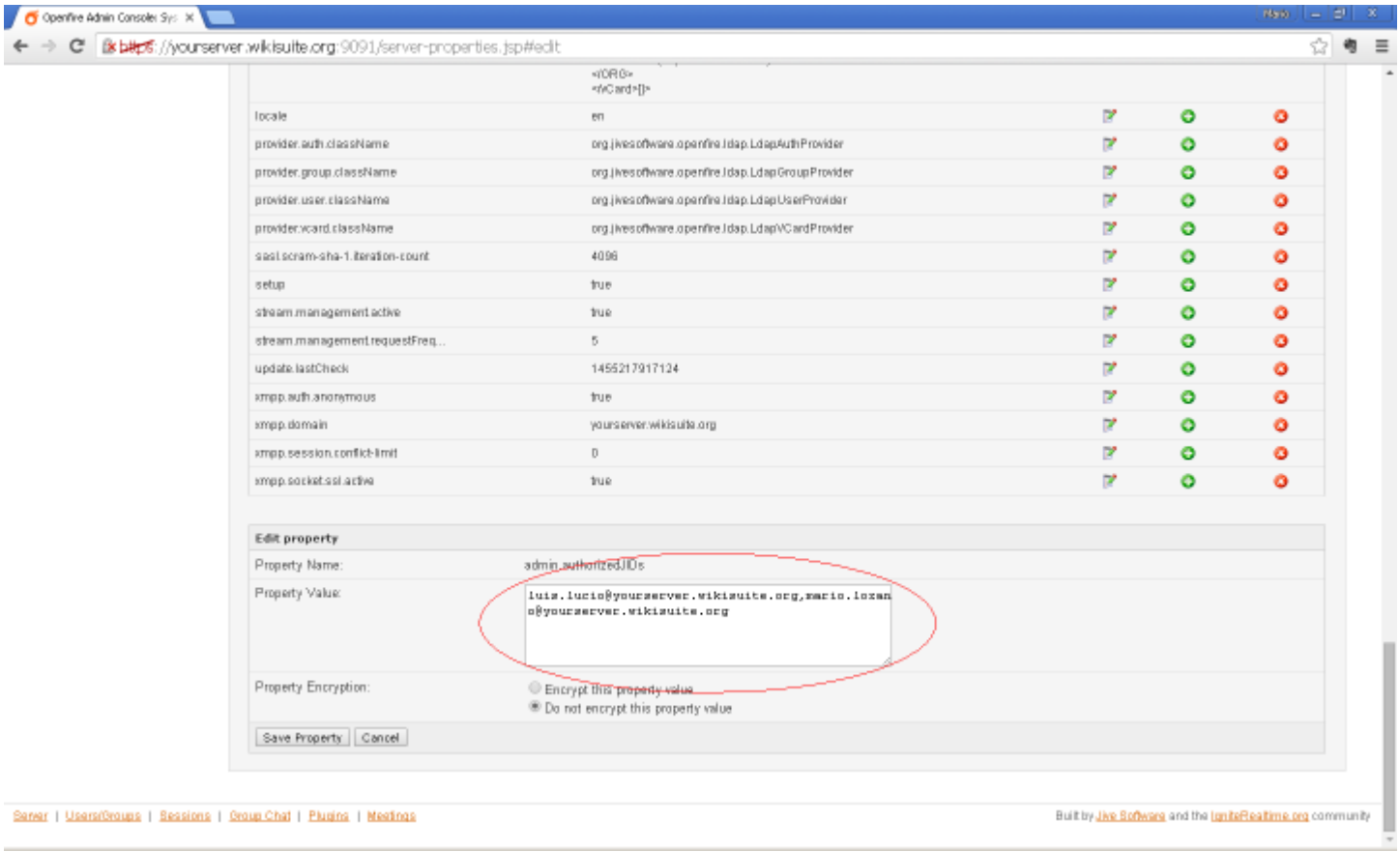
Currently, the Openfire clearos app only allows adding one admin user. As of this writing (2017-03-14), it will even clobber all other admins except the newly selected one if you change it.

1.-There is no ClearOS group for the Openfire admins. To add more admins, you need to go into the Openfire admin interface Server -> Server Manager -> System Properties -> admin.authorizedJIDs .

Edit server properties (https://yourserver.wikisuite.org:9091/server-properties.jsp).




2.- Find the admin.authorizedJIDs property, edit it and add comma-separated full JIDs. In our specific case user@example.org. "Click on Save Property".



3.- Openfire needs a restart. Log in to your ClearOS via SSH using root and type:

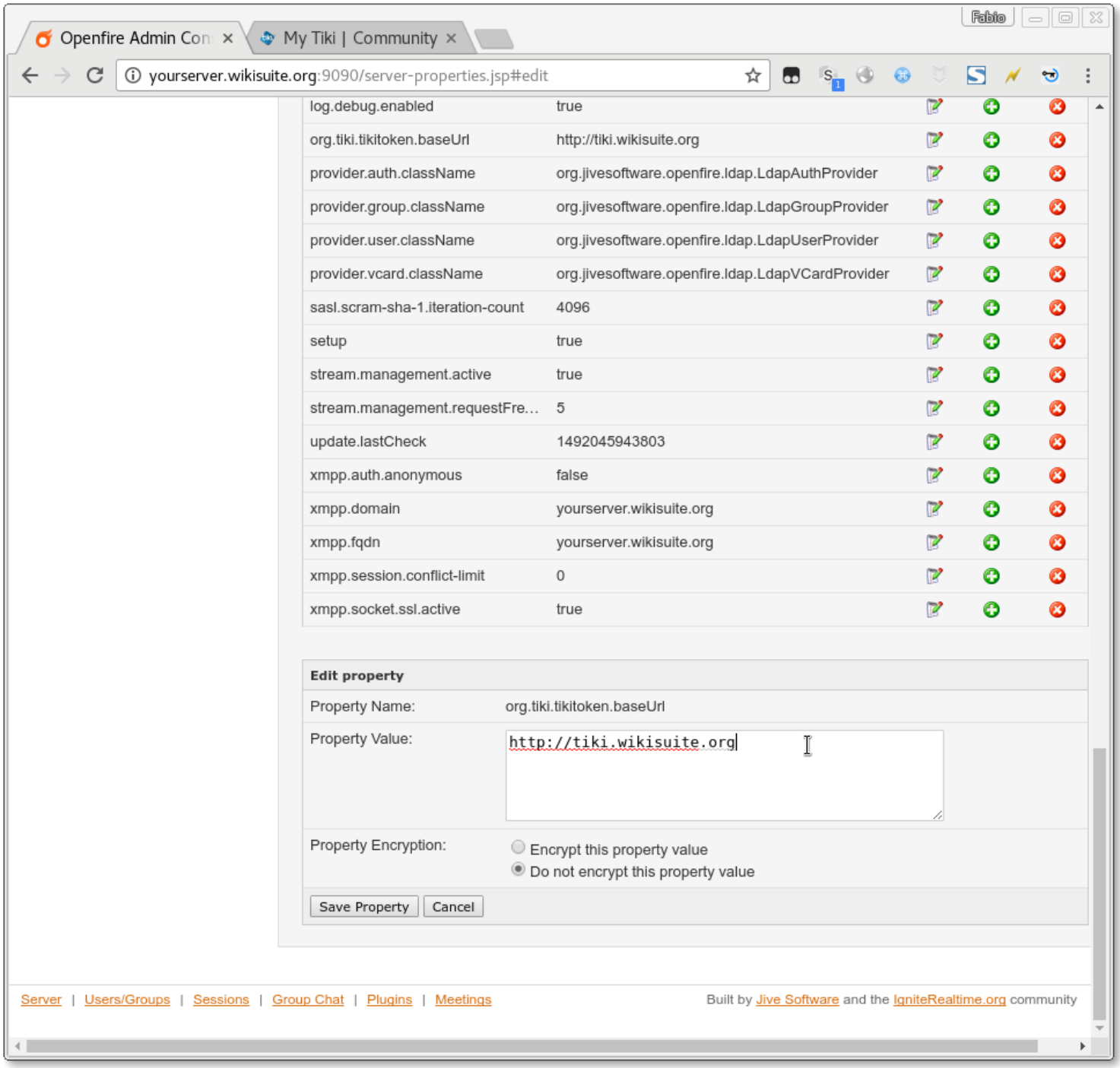
```
service openfire restart
```

# Configure Tiki, ConverseJS and OpenFire

To get a transparent authentication between ConverseJS and Openfire, we need to configure Tiki and install the TikiToken plugin (https://github.com/igniterealtime/openfire-tikitoken-plugin) in OpenFire.

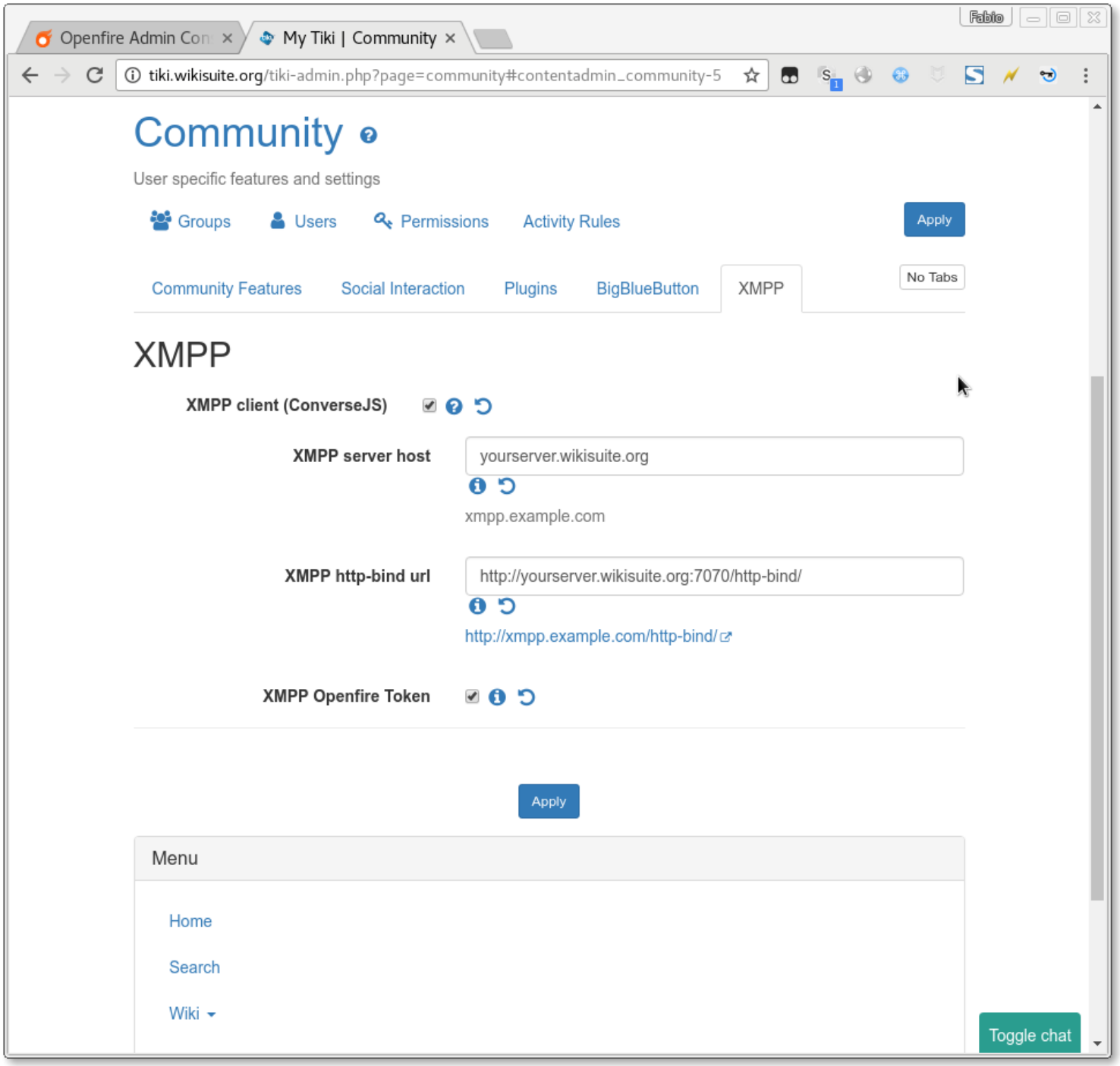
1 - The Tiki Token plugin is now shipping as an optional plugin in Openfire 4.1.5 Just activate as you would for any Openfire plugin. (You may also find more recent snapshots at Download the latest tikitoken.jar at https://github.com/igniterealtime/openfire-tikitoken-plugin/releases).

2 - Go to server properties page at http://yourserver.wikisuite.org:9090/server-properties.jsp and set up a new property with name **org.tiki.tikitoken.baseUrl** and property value will be your tiki base url; let's suppose **http://tiki.wikisuite.org**.




3 - Configure Tiki to talk to OpenFire. Go to the community page on the admin panels (RTC page on Tiki 19+), select the XMPP tab,
and:

- Check the **XMPP client (ConverseJS)**.
- On **XMPP server host** field, type **yourserver.wikisuite.org**.
- On **XMPP http-bind url** field, type https://yourserver.wikisuite.org:7070/http-bind/ .
- Check **XMPP Openfire Token**.
- Click on **Apply**.

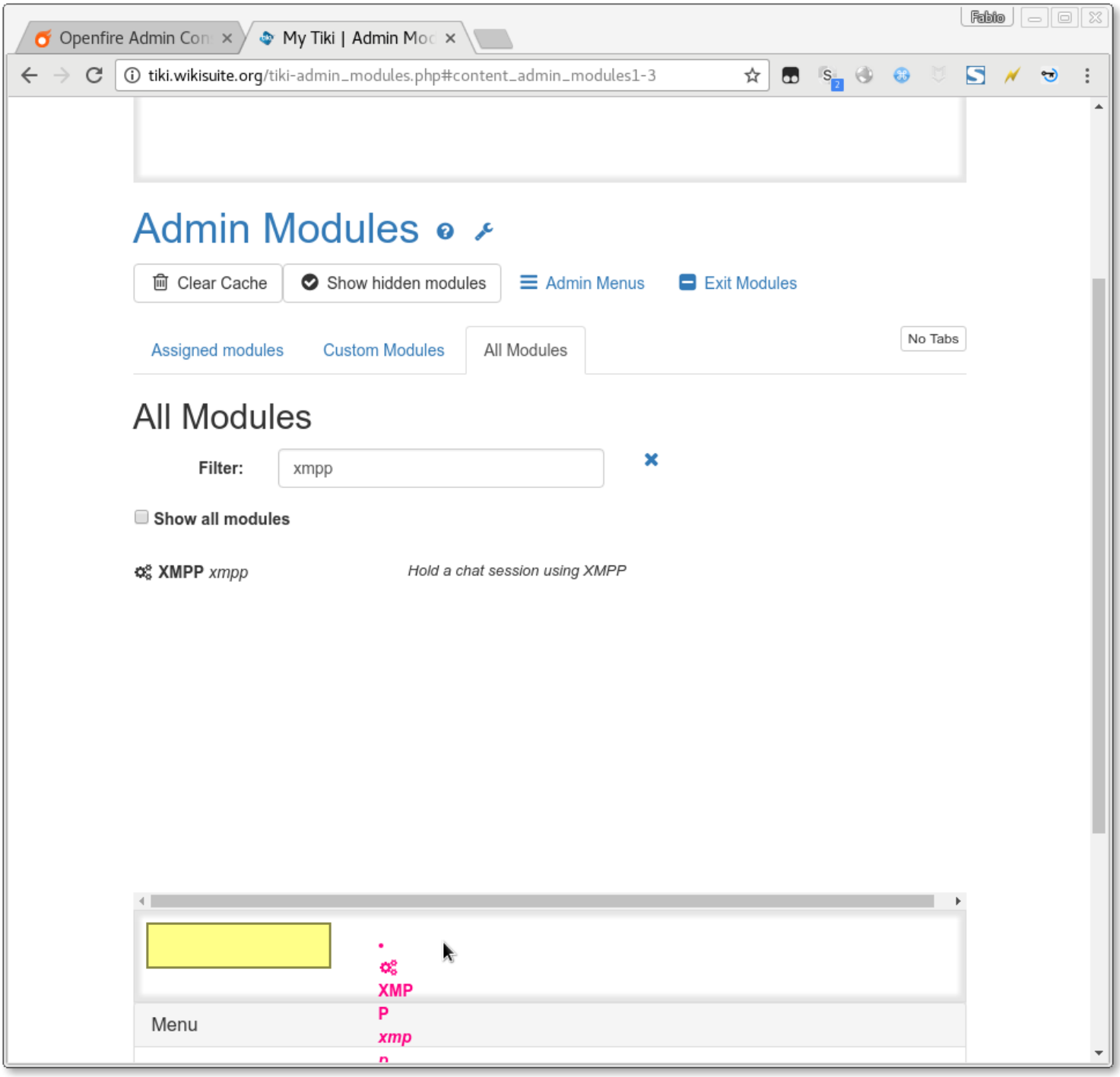



4 - Still on Tiki, go to the "Admin Modules" panel (http://tiki.wikisuite.org/tiki-admin_modules.php).

5 - Click on the "All modules" tab.

6 - On field **Filter** type xmpp .

7 - Drag the result to the bottom of the page, in the closest gray-bordered box.




8 - Just save and the popup will appear.

9 - Refresh the page to see the box at the bottom of the page.

Alternatively, you can put PluginXMPP in a wiki page (Tiki19+).

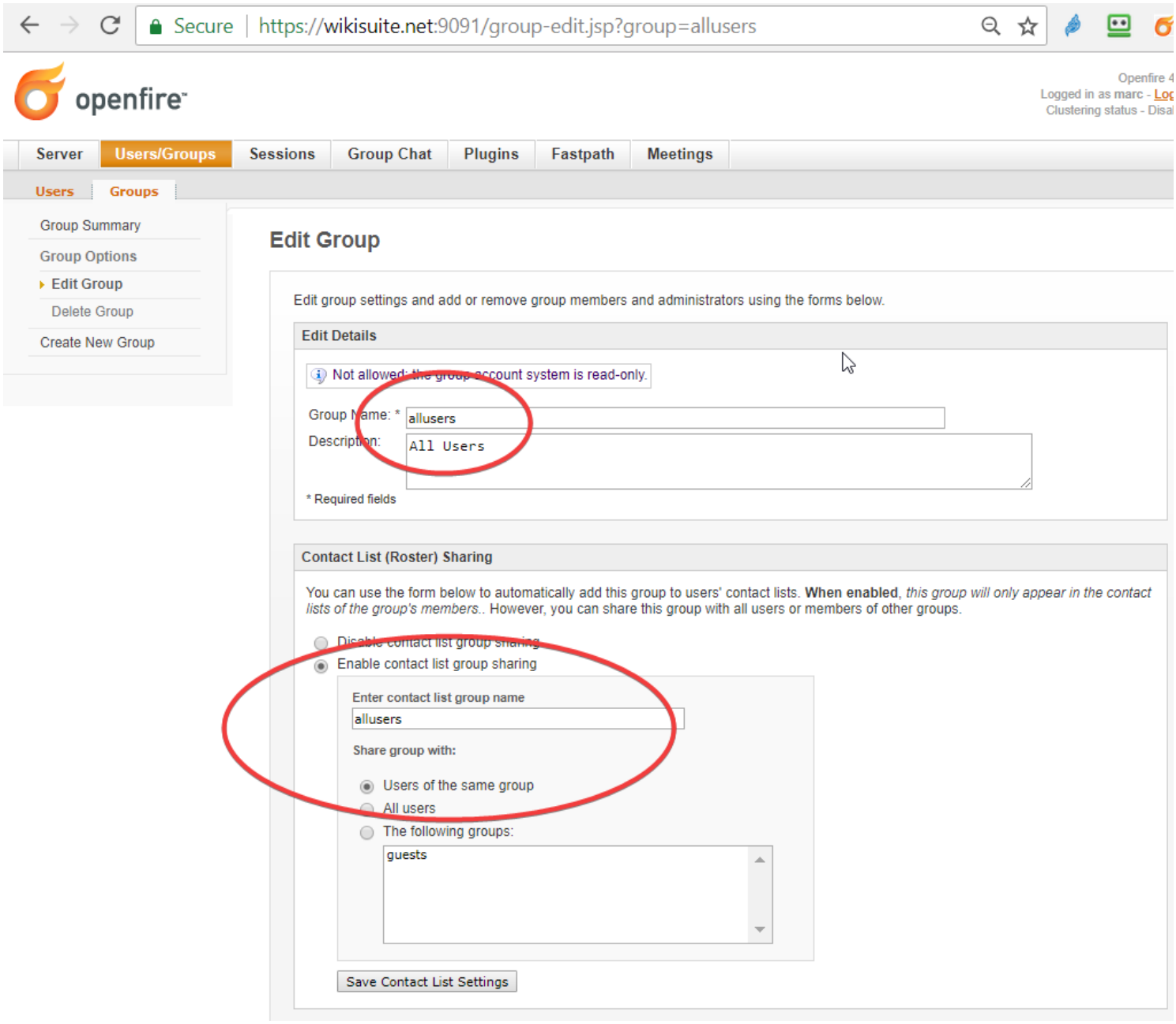
# Additional configuration

# File uploads

This needs to be activated (server-wide, not on a room-by-room basis). The only thing that needs to be done here is to install an Openfire plugin called "HTTP File Upload". Once it is installed, compliant clients will discover the availability of the feature, and start offering the related functionality.

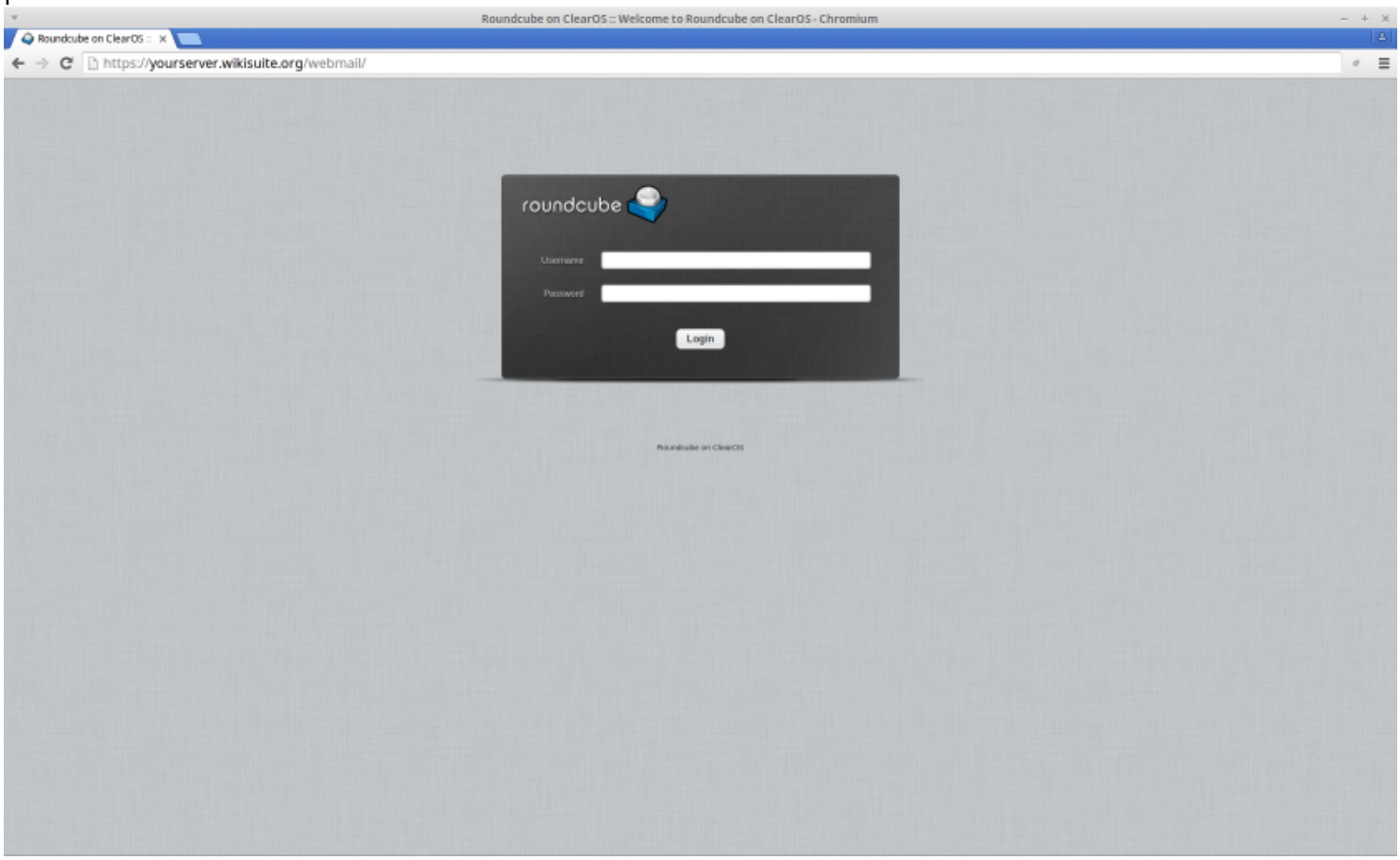
To install a plugin, log in to the Openfire admin console. Find the "Plugins" tab. If the "HTTP File Upload" plugin is not listed in the collection of installed plugins, click on "available plugins" in the left-hand side menu, and install the plugin.

# For everyone to see the status of everyone (Contact list group sharing)



# Configure email

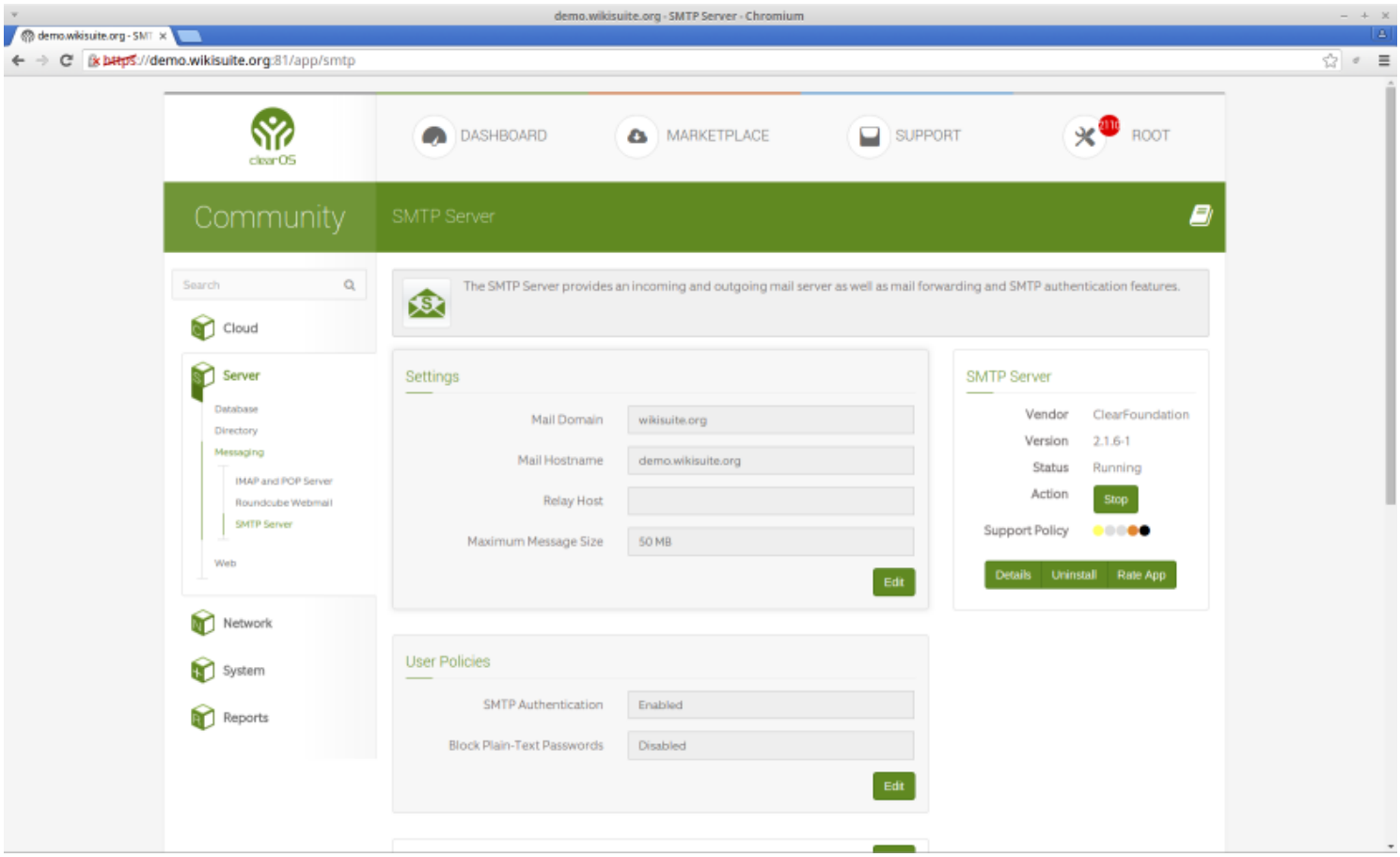
Go to https://yourserver.demo.wikisuite.org/webmail to access Roundcube, then log in with your username and password.




## In ClearOS

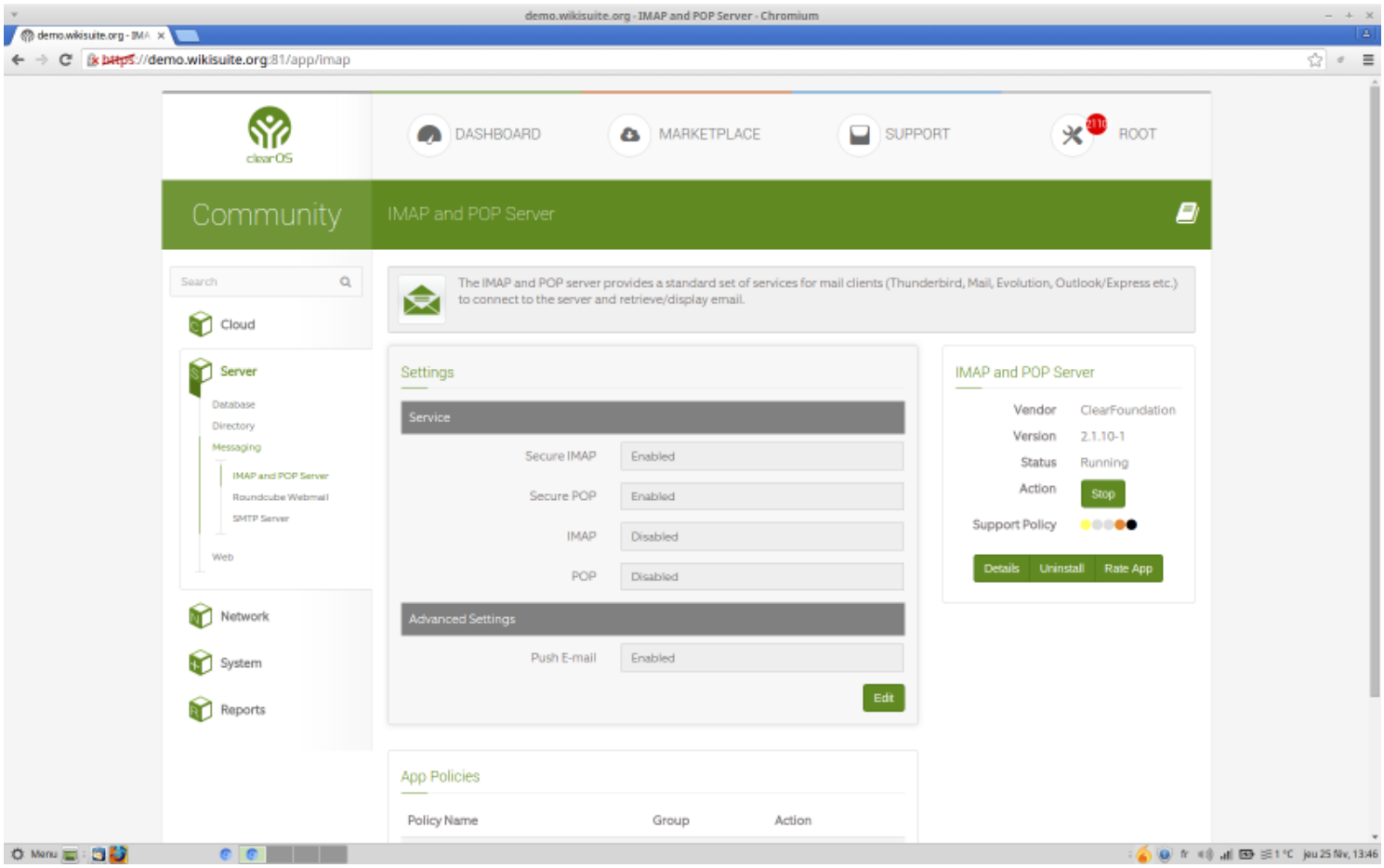
# Options about sending emails

https://example.org:81/app/smtp



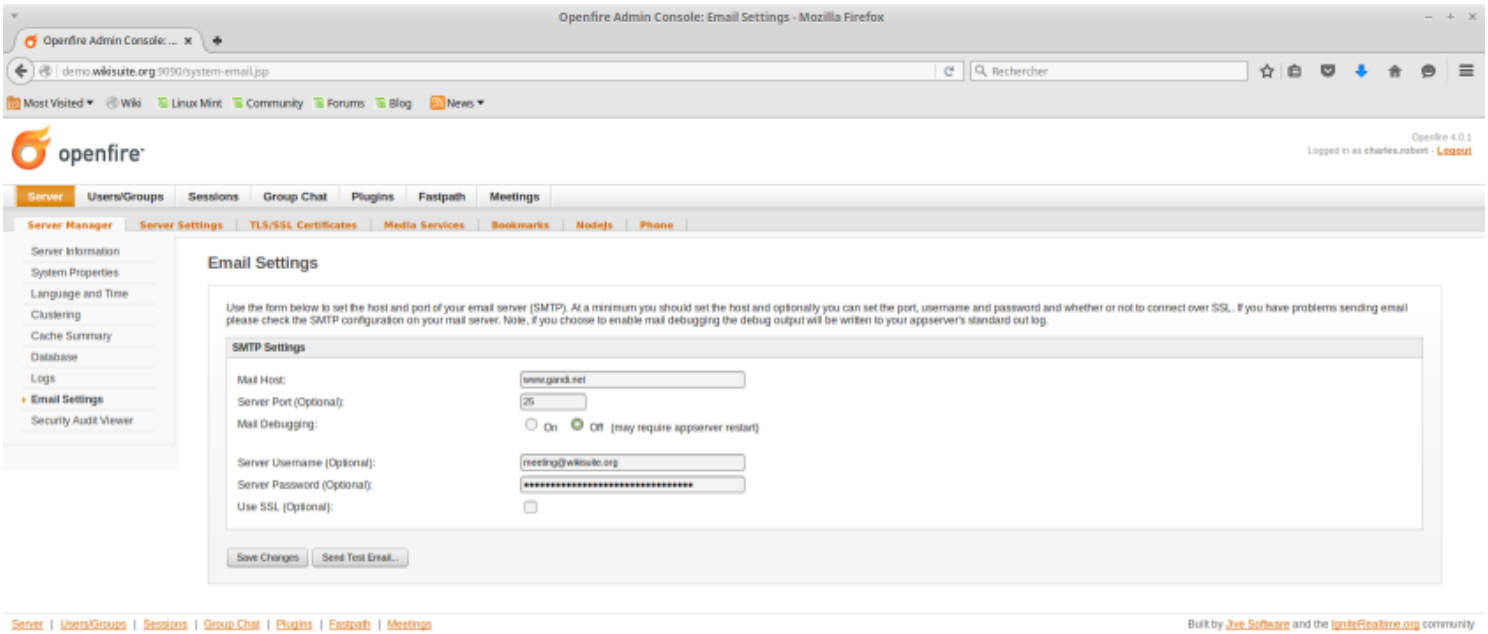

# Options about receiving emails

https://example.org:81/app/imap

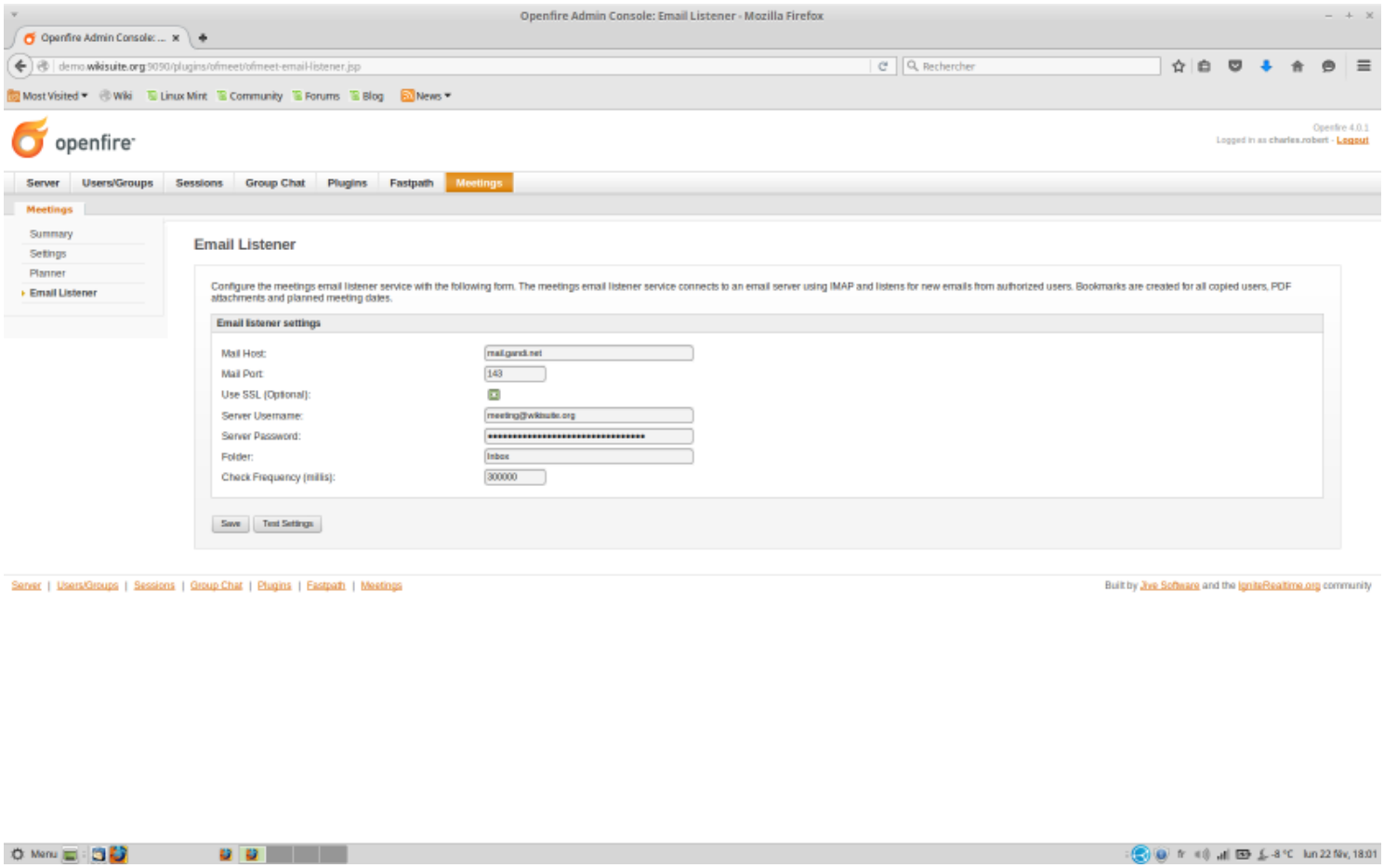



# In Openfire

Edit the email setting in the Server Manager tab as in the image:
https://example.org:9091/system-email.jsp




Edit the email listener in the Meeting tab as in the image:
https://example.org:9091/plugins/ofmeet/ofmeet-email-listener.jsp




# Avoiding non-standard ports

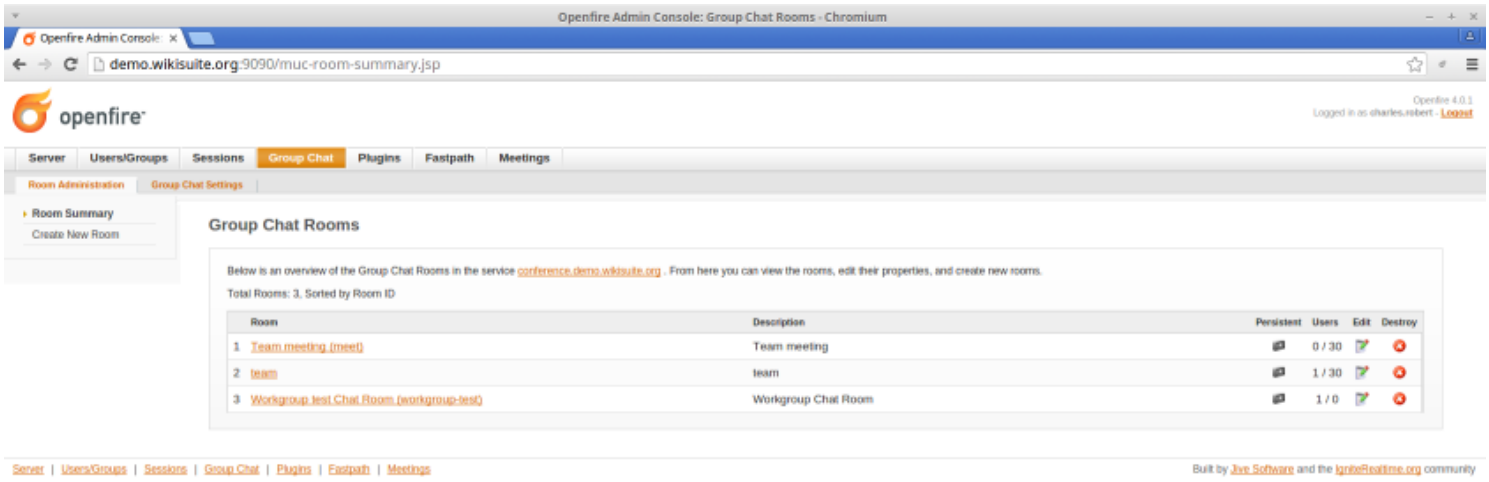
In some contexts, (corporate environments, captive portals in Internet cafes, etc.), some ports can be blocked. Thus, if you want to get rid of a port number, you can input the following apache configuration (Apache 2.4+ so you need ClearOS 7.x):

```
ProxyPass /ofmeet/ http://localhost:7070/ofmeet/
ProxyPassReverse /ofmeet/ http://localhost:7070/ofmeet/
ProxyPass /ofmeetws/ wss://localhost:7070/ofmeetws/
ProxyPassReverse /ofmeetws/ wss://localhost:7070/ofmeetws/
```

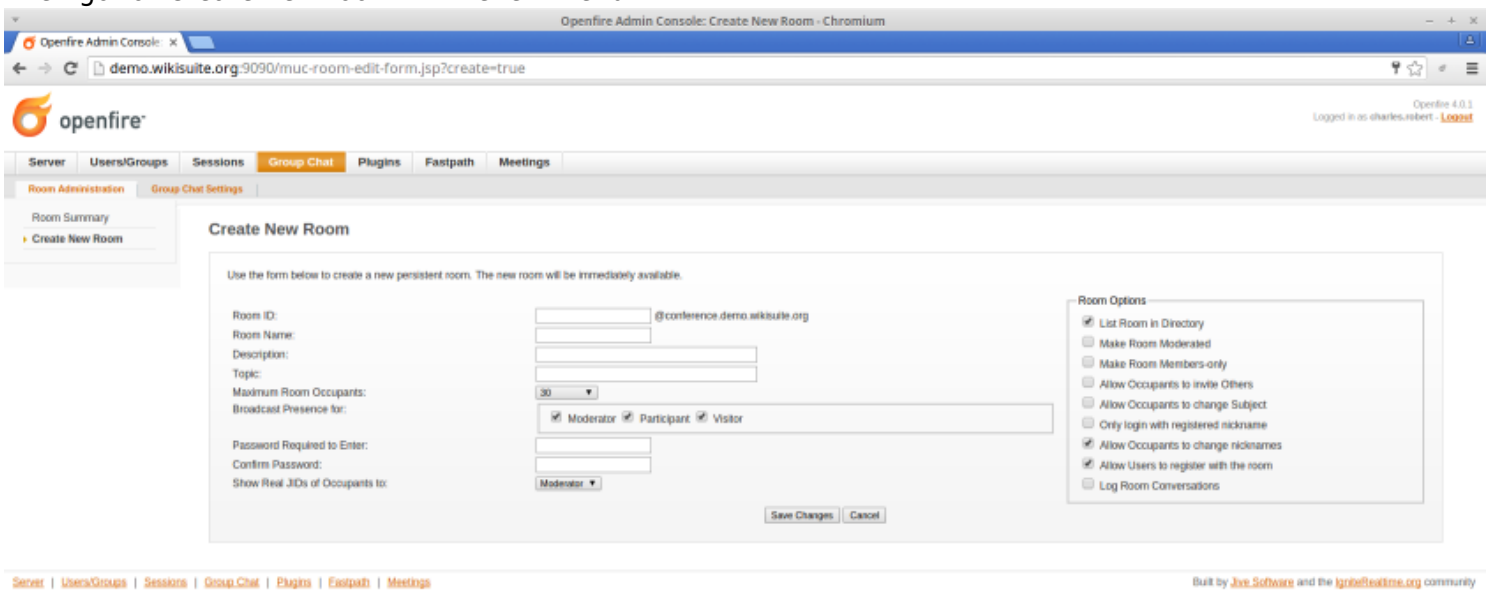
# Team room

## To create a private room

Go on "Group Chat" tab.




Then go to "Create new room" in the left menu.



Fill out the appropriate fields (Minimum Room ID, Room Name and Description). Finish by clicking on the Save Changes button.

## For use the private room

Note: This will be replaced by ConverseJS.

- Web access with CandyChat

Go to https://example.org:7443/ofmeet/candy.html
then log in with your account access.

- WebRTC access

With https://example.org:7443/ofmeet/ (from which you can pick a room)

- XMPP client access

with Spark in a login session, click on the "Action" tab, then the "Join a chatroom" option. In a new pop up, double-click in the list on the desired chatroom.
With Jitsi in a login session, click on the "File" tab, then the "Join a chatroom" option. In the new pop up, select the desired account and input a chatroom name.

# Call in and out of WebRTC conferences with a SIP account

- Requires OFMeet 0.9.5, which now has Jigasi: In Openfire's admin console, navigate to Meetings > Meetings > Gateway to SIP and fill out an account.

# Remote Control of Keyboard and Mouse

Nearly ready: https://github.com/igniterealtime/Pade/issues/24
This requires users to install an app on their desktop (Windows / GNU/Linux / MacOSX) and to have the Openfire plugin for Chrome.

## How to use

- You as the person who is actively sharing a screen can select the panel of a participant on the film strip. If video is **not** working, you will not get any video panels. If you do, then you can select any and then click on remote control icon. The person on the other end will be notified that they have control of your desktop
- You as a participant can request remote control of an active screenshare from the desktop owner by clicking on the remote control icon. The owner will receive a popup window requesting an accept or decline. If request is accepted, then remote control will be given.

# STUN / TURN server

- Todo later Marc: discuss with Dele (What / How to install and what ports to open)

# Advanced configuration

- If your XMPP server is not on the same server as your website, and you want to support (typically older) XMPP clients which don't support SRV records, you will need something like http://sourceforge.net/p/penloadbalancer/wiki/penctl.1/

# Pàdé XMPP client

Please see Pàdé

## Todo: Make sure these installation instructions provide great security

- Secure by default. Remove all http, and force https.
- Ref: http://wiki.xmpp.org/web/Securing_XMPP#Openfire
- Not like this: IM Observatory Test.
- Verify that documenting leads to respecting Public Statement Regarding Ubiquitous Encryption on the XMPP Network.

# Related links

- http://igniterealtime.org/projects/openfire/documentation.jsp
- https://www.clearos.com/clearfoundation/social/community/how-to-install-openfire-3-7-1-on-cos-6-3-64bit-manual-install
- http://rtcquickstart.org/guide/RTCQuickStartGuide.pdf
- How to install Spark

# Souce code

| Source | Packages |
|---|---|
| https://github.com/WikiSuite/app-openfire | http://koji.clearos.com/koji/packageinfo?packageID=303 |
| https://github.com/WikiSuite/app-openfire-plugin | http://koji.clearos.com/koji/packageinfo?packageID=311 |
| https://github.com/WikiSuite/openfire | http://koji.clearos.com/koji/packageinfo?packageID=302 |

# Troubleshooting

## Changing Openfire configuration when you can't log in to the system database

Openfire stores its configuration in the database. On ClearOS, that is the system database.

Getting into the ClearOS system database can be a little confusing the first time. ClearOS typically runs two database servers. You will need the system database root password, and to connect to a non-default socket. Here is how:

```
cat /var/clearos/system_database/reports
mysql -u root openfire -p --socket /var/lib/system-mysql/mysql.sock
```

You can then edit the Openfire configuration, which is stored in the ofProperty table. (SELECT * FROM `ofProperty`)

One change you are likely to want to make during debugging is to enable ldap debugging

```
INSERT INTO `openfire`.`ofProperty` (`name`, `propValue`, `encrypted`) VALUES
('log.debug.enabled', 'true', NULL);
exit
service openfire restart
tail -f /var/log/openfire/debug.log
```

Useful references:
* Openfire LDAP guide
* ClearOS: Re-initialize your LDAP directory

## It used to work, but I just lost access when I installed the Directory app.

The problem is most likely that your base domain changed.

OpenLdap on base ClearOS creates domains of the form:

dc=system,dc=lan

Unfortunately, if you install the ClearOS directory app AFTER Openfire, your base domain is likely to change. It's going to be:
If "Base Domain" is your.domain.name,
your base DN will be:
dc=your,dc=domain,dc=name

Openfire will not update its configuration automatically. You'll have to update the following ofProperty in

Openfire's database
* ldap.baseDN (as is)
* ldap.searchFilter (modify the value in the parenthesis as appropriate)

## Testing OpenLDAP from the command line

This should work:

```
ldapsearch -x -h localhost -b 'dc=your,dc=domain,dc=name' 'uid=your_openfire_admin_user'
```

If the above does not return your user, logging into the Openfire admin console will NOT work.

This may help diagnose:

```
ldapsearch -x -h localhost
```

Should list all users. If you don't see yours, something is really wrong with your ldap configuration.

alias

- How to install and Configure Openfire Meetings on ClearOS