

# 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 Thus, the information below is no longer updated.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

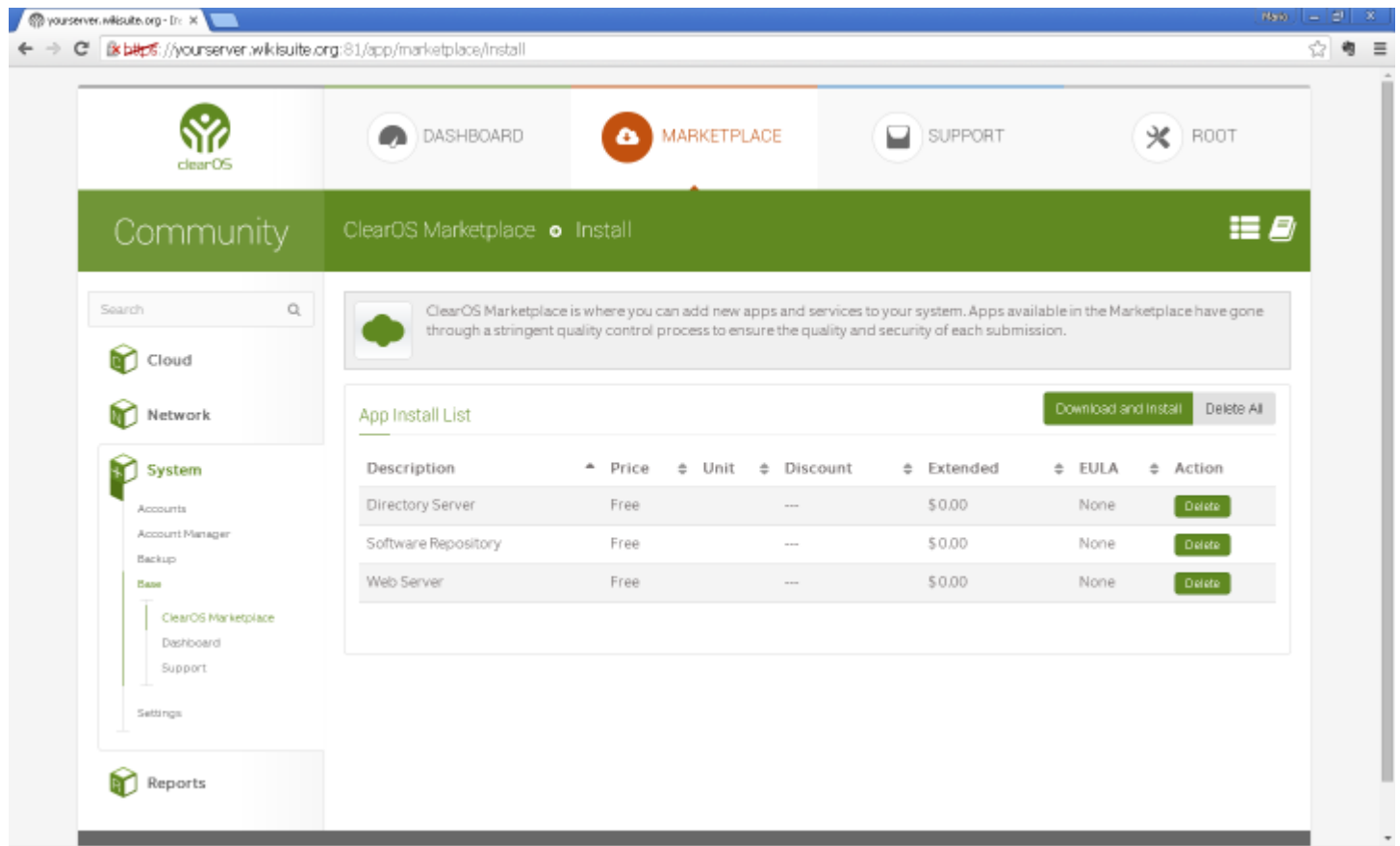
## Assumptions

- 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](#)

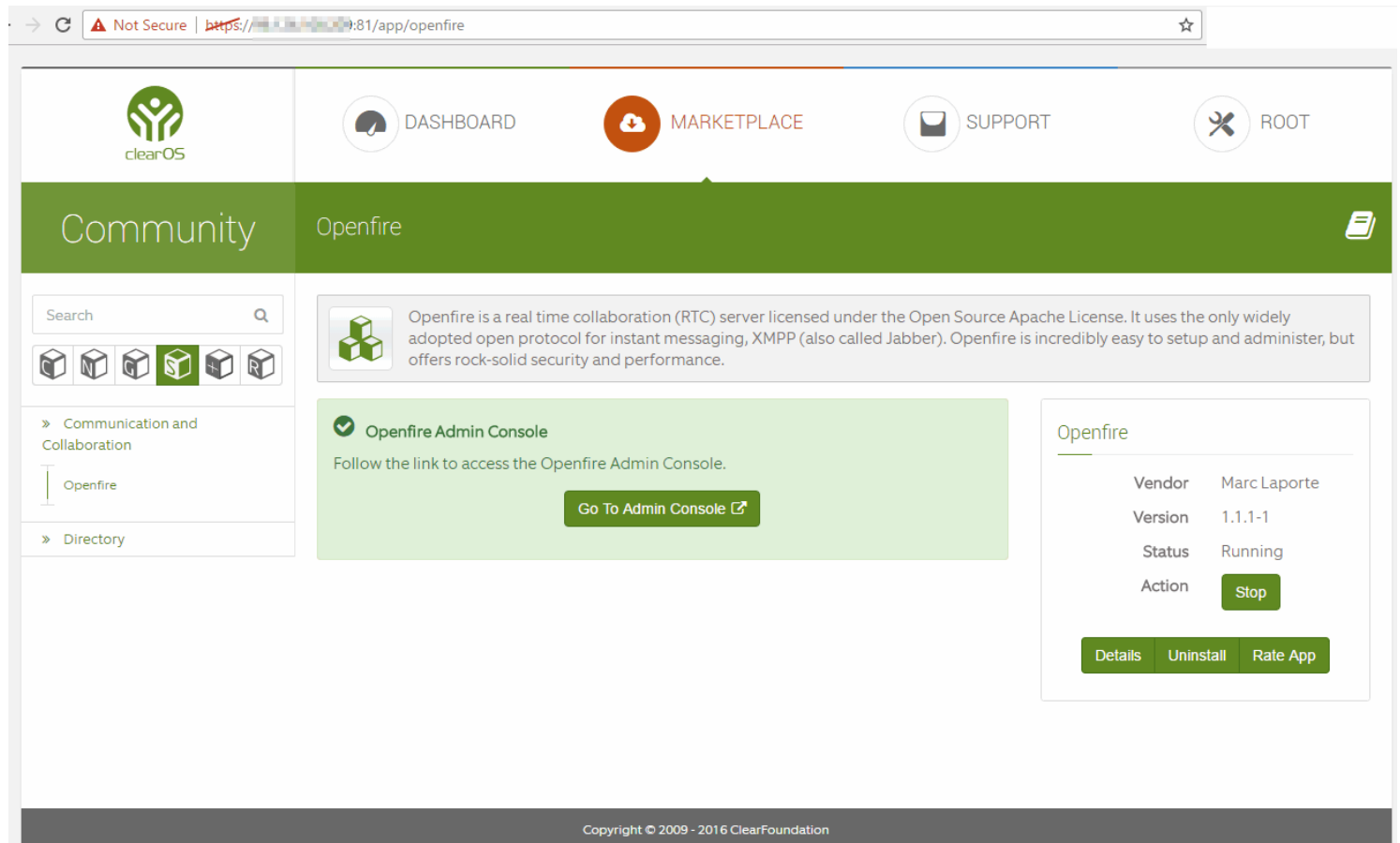
## Install Openfire

- 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](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](https://yourserver.wikisuite.org:81/app/openldap_directory/settings/edit)).

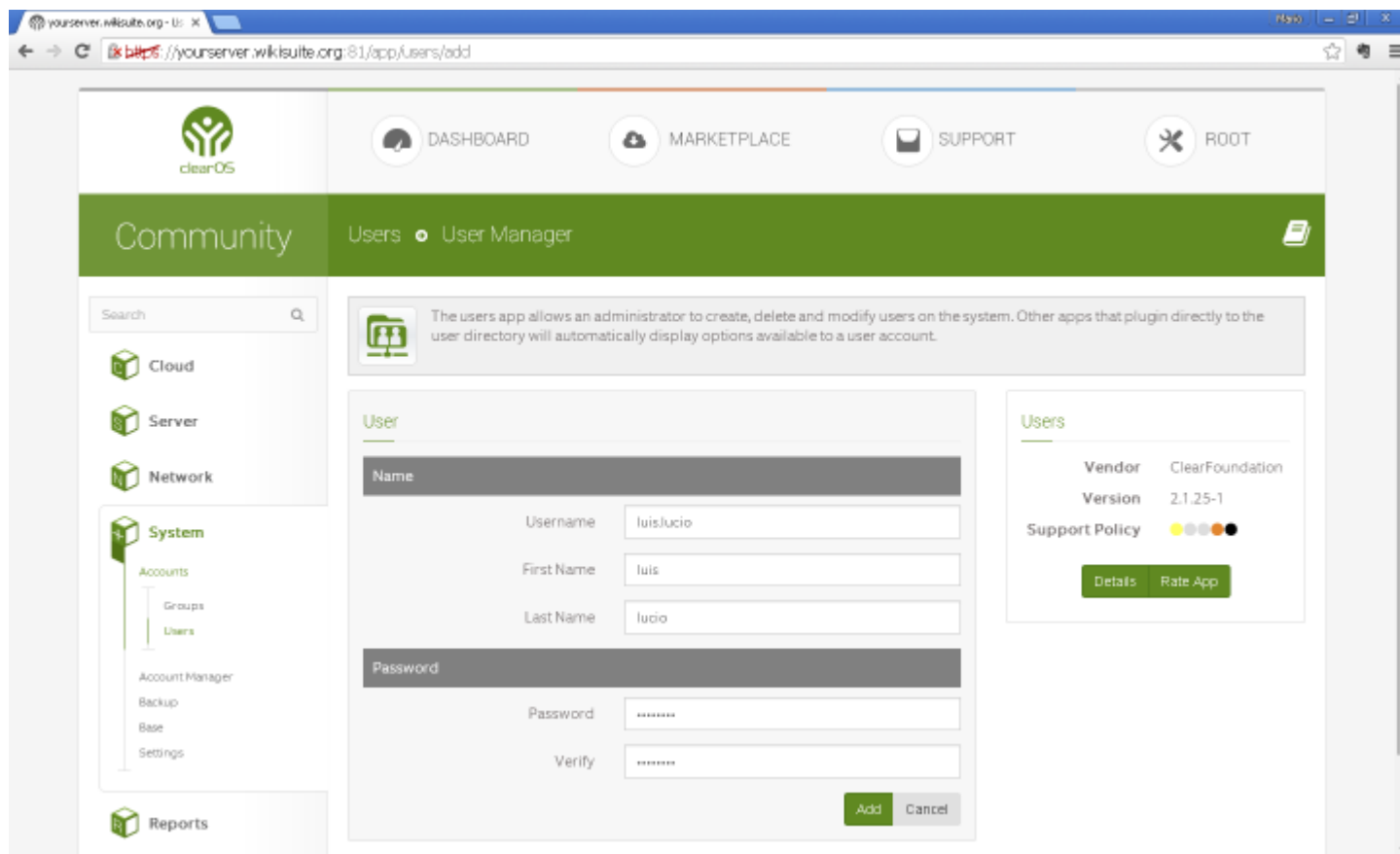
File not found.

- 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](https://yourserver.wikisuite.org:81/app/openldap_directory/policies/edit)).

File not found.

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

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.

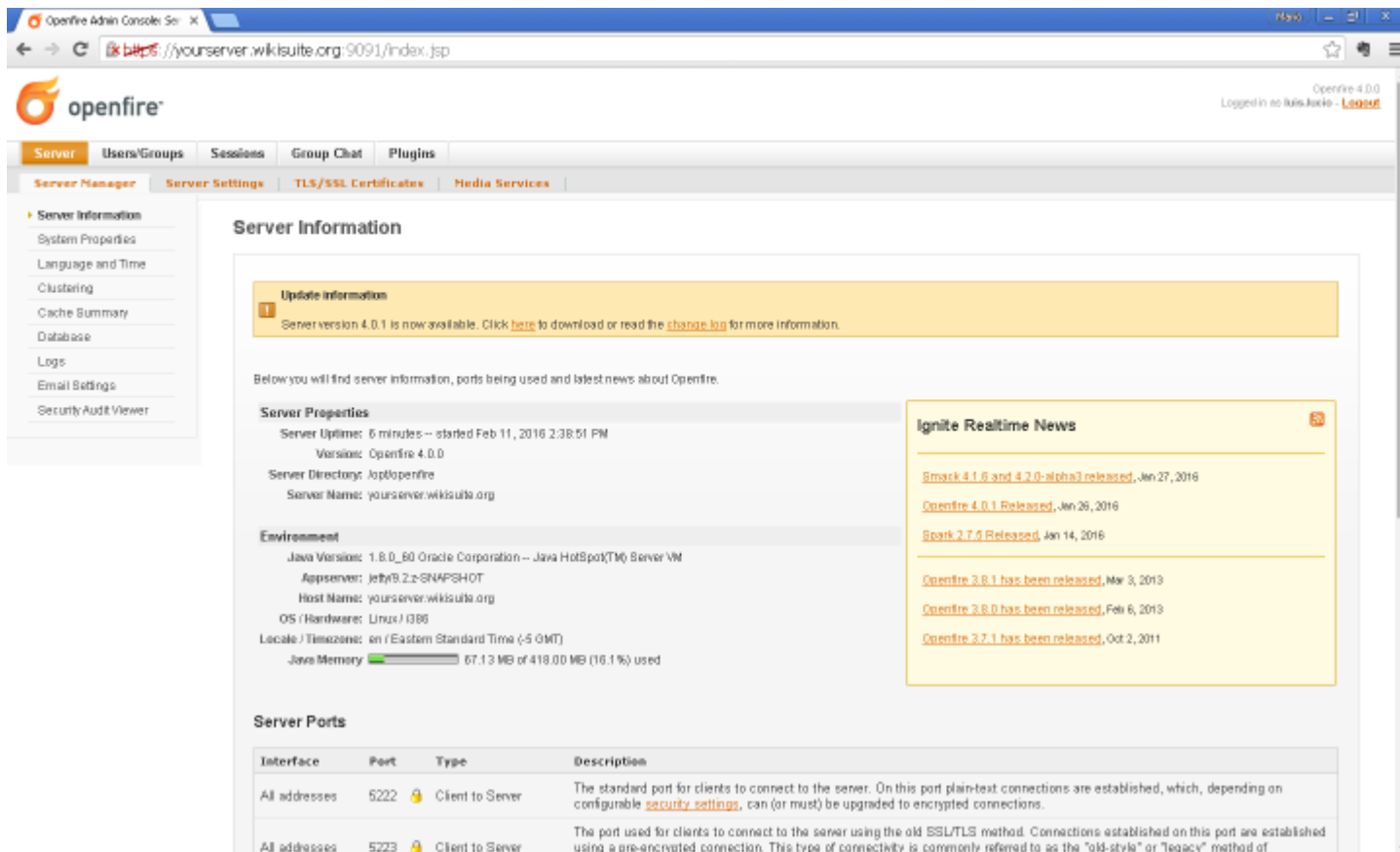
## Configure Openfire

**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.ignite realtime.org/builds/openfire/docs/latest/documentation/install-guide.html>



The screenshot displays the Openfire Admin Console interface. The top navigation bar includes tabs for Server, Users/Groups, Sessions, Group Chat, and Plugins. The left sidebar lists various server management options. The main content area is titled 'Server Information' and contains several sections: 'Update Information' with a notification about version 4.0.1, 'Server Properties' showing uptime and version details, 'Environment' with system specifications, 'Server Ports' table, and 'Ignite Realtime News' with release announcements.

Interface	Port	Type	Description
All addresses	5222	Client to Server	The standard port for clients to connect to the server. On this port plain-text connections are established, which, depending on configurable <a href="#">security settings</a> , can (or must) be upgraded to encrypted connections.
All addresses	5223	Client to Server	The port used for clients to connect to the server using the old 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

## 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)

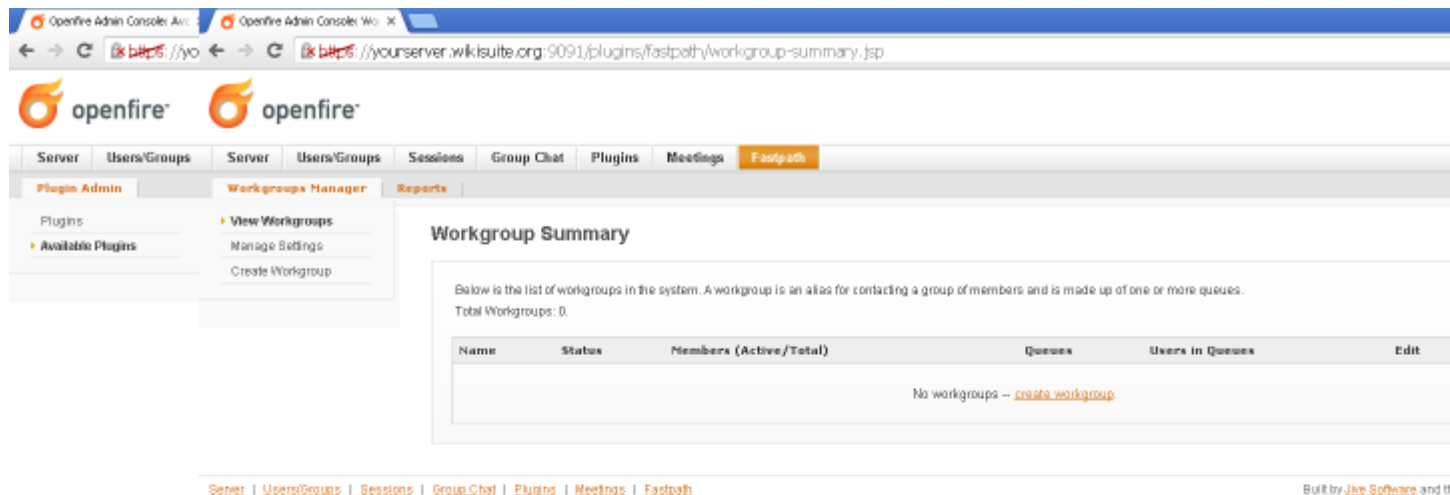
## Configure Openfire Meetings Plugin

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>).



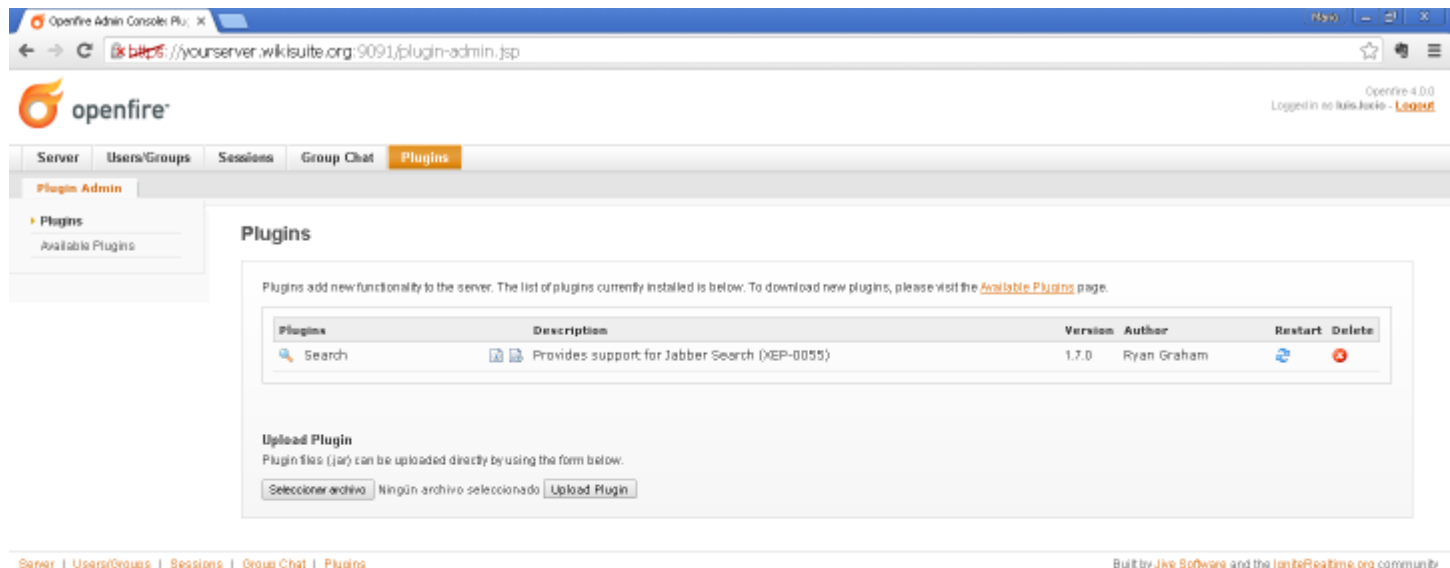


## Notes:

- 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



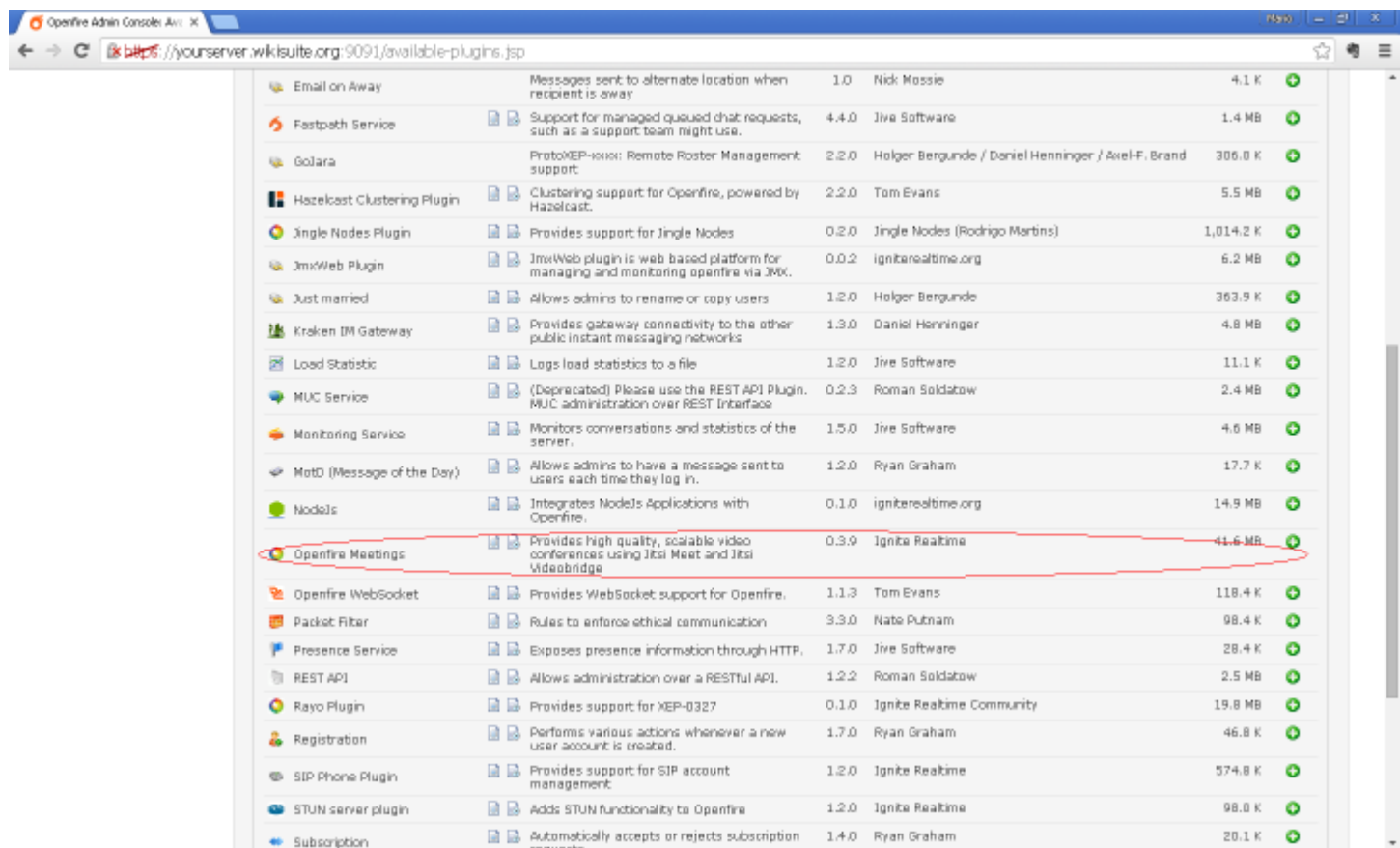
The screenshot shows the Openfire Admin Console interface. The top navigation bar includes links for Server, Users/Groups, Sessions, Group Chat, and Plugins. The Plugins section is active, showing a list of installed plugins. Below the list is an 'Upload Plugin' section with a file input and an 'Upload Plugin' button. The browser address bar shows the URL: <http://yourserver.wikisuite.org:9091/plugin-admin.jsp>.

Plugins	Description	Version	Author	Restart	Delete
Search	Provides support for Jabber Search (XEP-0055)	1.7.0	Ryan Graham		

**Upload Plugin**  
Plugin files (.jar) can be uploaded directly by using the form below.

Ningún archivo seleccionado

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

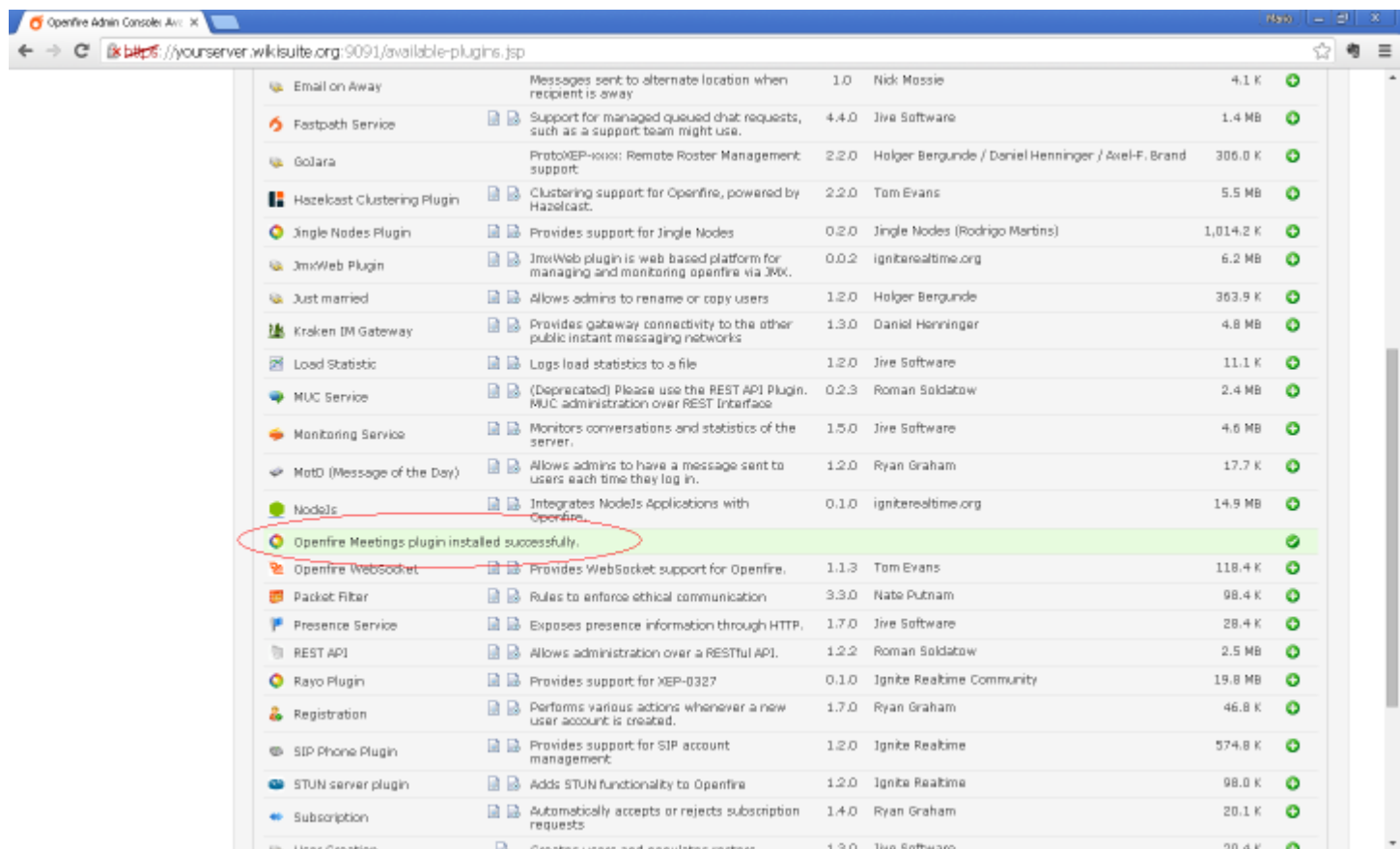


The screenshot shows the Openfire Admin Console interface with the 'Available Plugins' section active. A list of available plugins is displayed, including details like name, description, version, author, and size. The 'Openfire Meetings' plugin is highlighted with a red circle.

Plugin	Description	Version	Author	Size	Action
Email on Away	Messages sent to alternate location when recipient is away	1.0	Nick Mossie	4.1 K	
Fastpath Service	Support for managed queued chat requests, such as a support team might use.	4.4.0	Jive Software	1.4 MB	
Golara	ProtoJEP-1000: Remote Roster Management support	2.2.0	Holger Bergunde / Daniel Henninger / Axel-F. Brand	306.0 K	
Hazelcast Clustering Plugin	Clustering support for Openfire, powered by Hazelcast.	2.2.0	Tom Evans	5.5 MB	
Jingle Nodes Plugin	Provides support for Jingle Nodes	0.2.0	Jingle Nodes (Rodrigo Martins)	1,014.2 K	
JmxWeb Plugin	JmxWeb plugin is web based platform for managing and monitoring openfire via JMX.	0.0.2	ignite realtime.org	6.2 MB	
Just married	Allows admins to rename or copy users	1.2.0	Holger Bergunde	363.9 K	
Kroken IM Gateway	Provides gateway connectivity to the other public instant messaging networks	1.3.0	Daniel Henninger	4.8 MB	
Load Statistic	Logs load statistics to a file	1.2.0	Jive Software	11.1 K	
MUC Service	(Deprecated) Please use the REST API Plugin. MUC administration over REST interface	0.2.3	Roman Soldatow	2.4 MB	
Monitoring Service	Monitors conversations and statistics of the server.	1.5.0	Jive Software	4.6 MB	
MotD (Message of the Day)	Allows admins to have a message sent to users each time they log in.	1.2.0	Ryan Graham	17.7 K	
Node.js	Integrates Node.js Applications with Openfire.	0.1.0	ignite realtime.org	14.9 MB	
<b>Openfire Meetings</b>	<b>Provides high quality, scalable video conferences using Jitsi Meet and Jitsi Videobridge</b>	<b>0.3.9</b>	<b>Ignite Realtime</b>	<b>44.6 MB</b>	
Openfire WebSocket	Provides WebSocket support for Openfire.	1.1.3	Tom Evans	118.4 K	
Packet Filter	Rules to enforce ethical communication	3.3.0	Nate Putnam	98.4 K	
Presence Service	Exposes presence information through HTTP.	1.7.0	Jive Software	28.4 K	
REST API	Allows administration over a RESTful API.	1.2.2	Roman Soldatow	2.5 MB	
Rayo Plugin	Provides support for XEP-0327	0.1.0	Ignite Realtime Community	19.8 MB	
Registration	Performs various actions whenever a new user account is created.	1.7.0	Ryan Graham	46.8 K	
SIP Phone Plugin	Provides support for SIP account management.	1.2.0	Ignite Realtime	574.8 K	
STUN server plugin	Adds STUN functionality to Openfire	1.2.0	Ignite Realtime	98.0 K	
Subscription	Automatically accepts or rejects subscription requests	1.4.0	Ryan Graham	20.1 K	

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

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>).

Openfire Admin Console: Sys

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

Openfire 4.0.1  
Logged in as Luis Lucio - Logout

Server Users/Groups Sessions Group Chat Plugins Meetings

Server Manager Server Settings TLS/SSL Certificates Media Services

Server Information  
System Properties  
Language and Time  
Clustering  
Cache Summary  
Database  
Logs  
Email Settings  
Security Audit Viewer

### System Properties

Below is a list of the system properties. Values for encrypted and sensitive fields are hidden. Long property names and values are clipped. Hold your mouse over the property name to see the full value or to see both the full name and value, click the edit icon next to the property.

Property Name	Property Value	Edit	Encrypt	Delete
admin.authorizedJIDs	luis.lucio@yourserver.wikisuite.org,mario.lozano@y...			
adminConsole.port	9090			
adminConsole.securePort	9091			
connectionProvider.className	org.jivesoftware.database.EmbeddedConnectionPro...			
ldap.adminDN	/cn=admin			
ldap.adminPassword	/cn=admin			
ldap.autoFollowAliasReferrals	true			
ldap.autoFollowReferrals	false			
ldap.baseDN	dc=wikisuite,dc=org			
ldap.connectionPoolEnabled	true			
ldap.debugEnabled	false			
ldap.emailField	mail			
ldap.encodeDNs	true			
ldap.groupDescriptionField	description			
ldap.groupMemberField	member			
ldap.groupNameField	cn			
ldap.host	localhost			

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".

Openfire Admin Console: Sys

https://yourserver.wikisuite.org:9091/server-properties.jsp#edit

locale	en			
provider.auth.className	org.jivesoftware.openfire.ldap.LdapAuthProvider			
provider.group.className	org.jivesoftware.openfire.ldap.LdapGroupProvider			
provider.user.className	org.jivesoftware.openfire.ldap.LdapUserProvider			
provider.xcard.className	org.jivesoftware.openfire.ldap.LdapVCARDProvider			
ssl.scrum-sha-1.iteration-count	4096			
setup	true			
stream.management.active	true			
stream.management.requestFreq...	5			
update.lastCheck	1455217917124			
xmpp.auth.anonymous	true			
xmpp.domain	yourserver.wikisuite.org			
xmpp.session.conflict-limit	0			
xmpp.socket.ssl.active	true			

**Edit property**

Property Name: admin.authorizedJIDs

Property Value: luis.lucio@yourserver.wikisuite.org,mario.lozano@yourserver.wikisuite.org

Property Encryption:  
☐ Encrypt this property value  
☒ Do not encrypt this property value

Save Property Cancel

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

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

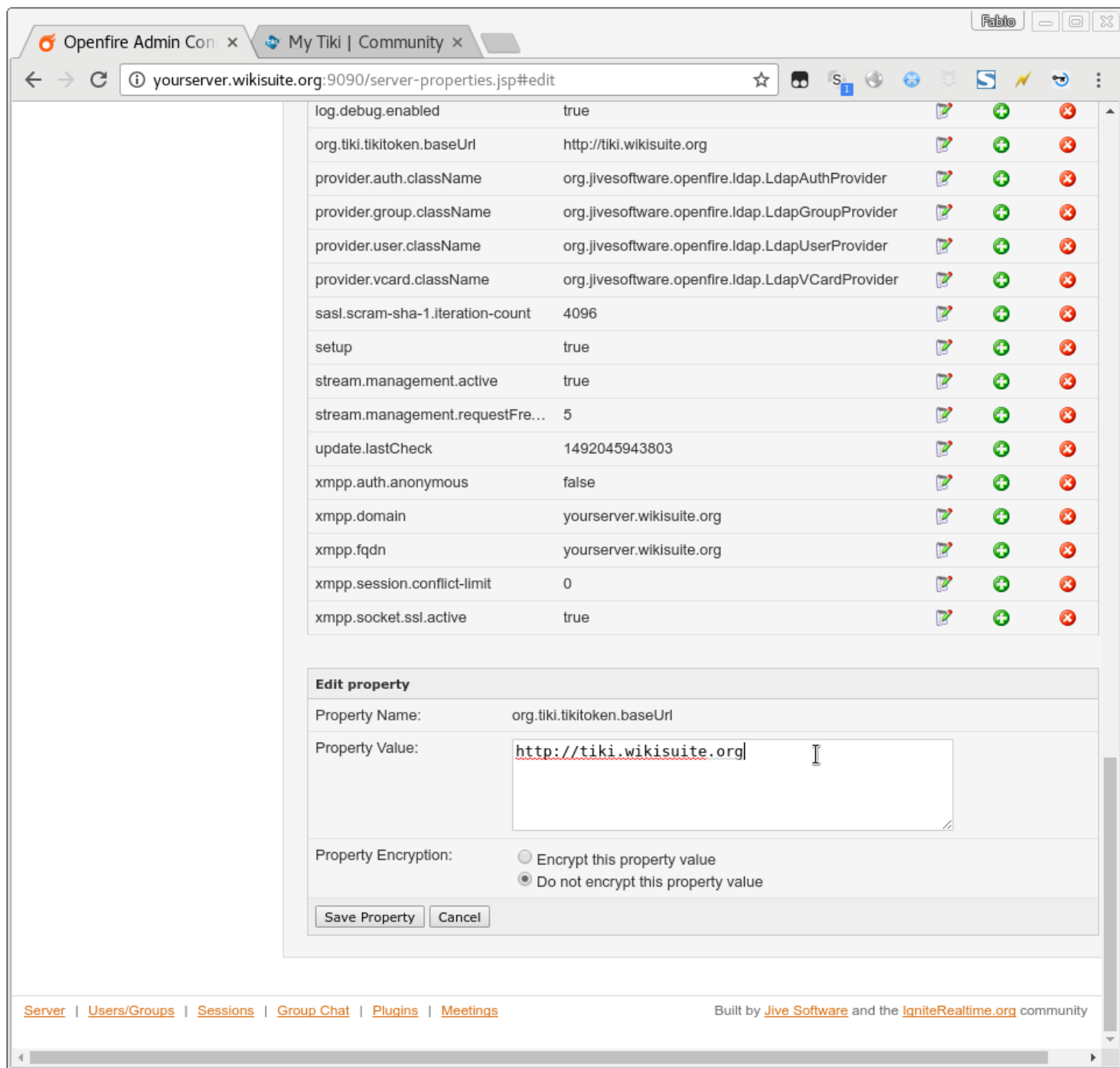
```
service openfire restart
```

## 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.

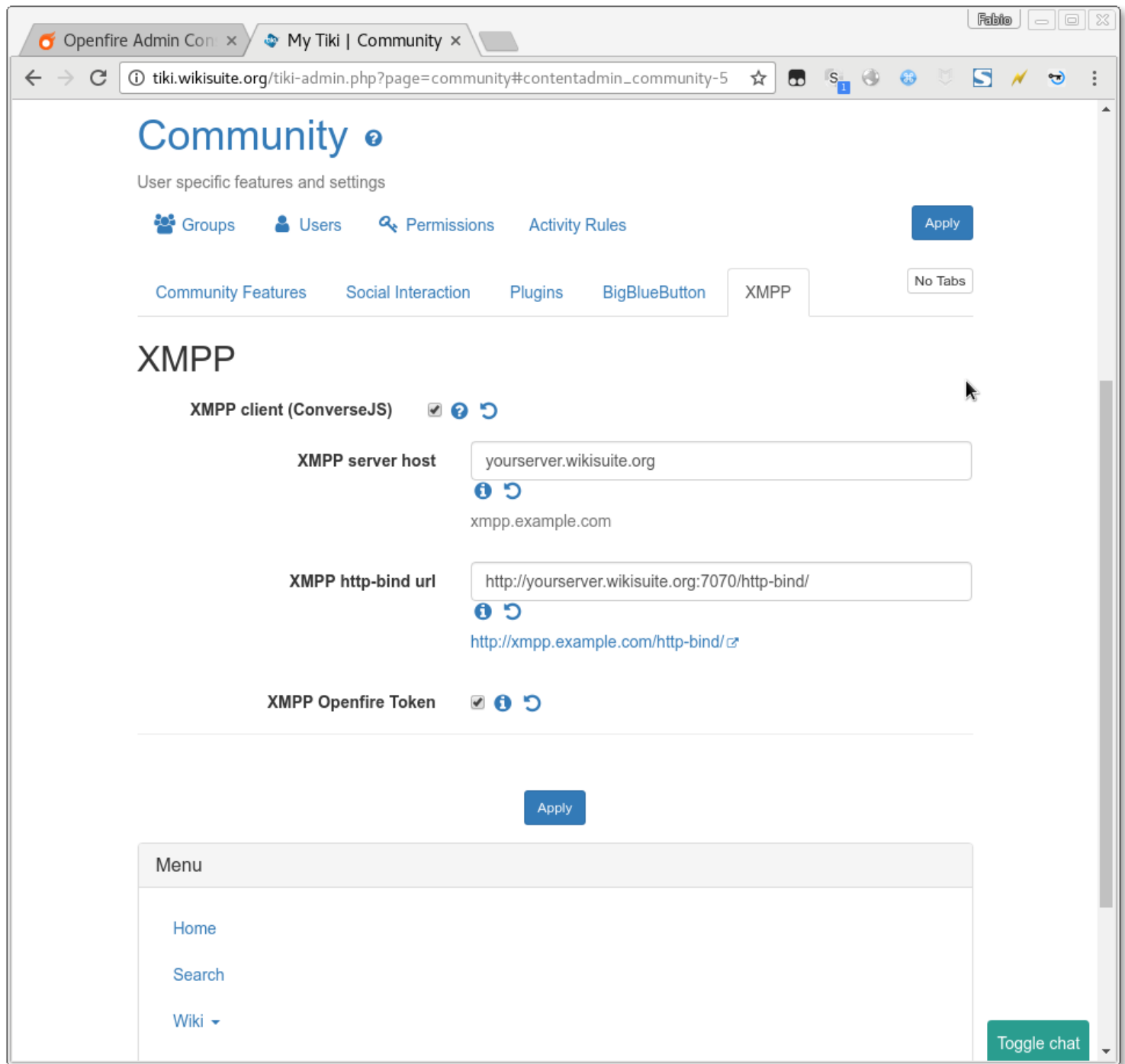
1 - The Tiki Token plugin is now shipping as an optional plugin in Openfire 4.1.5 Just activate as you would for any Openfire plugin. (You may also find more recent snapshots at Download the latest tikitoken.jar at <https://github.com/igniterealtime/openfire-tikitoken-plugin/releases>).

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**.

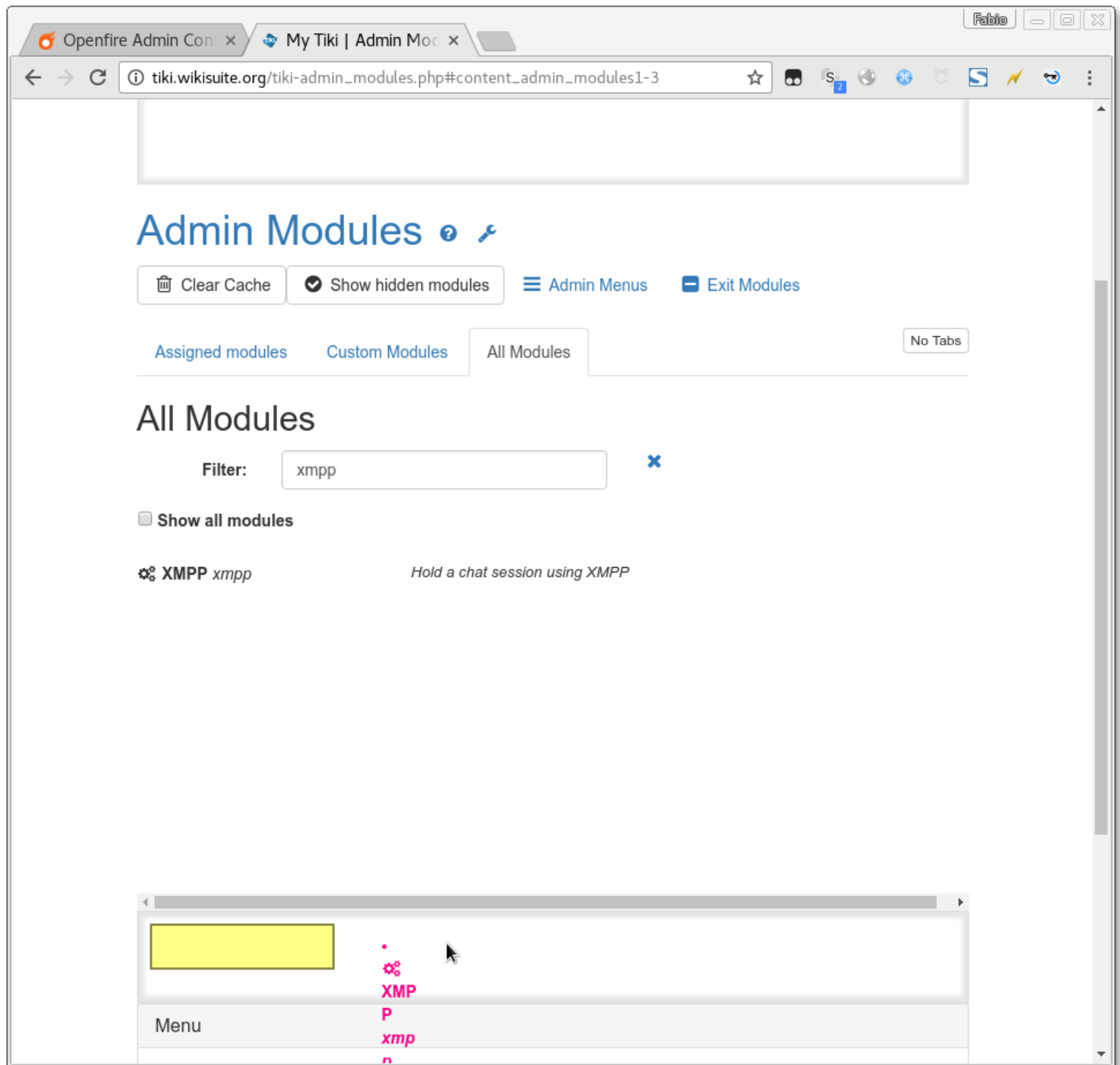


4 - Still on Tiki, go to the "Admin Modules" panel ([http://tiki.wikisuite.org/tiki-admin\\_modules.php](http://tiki.wikisuite.org/tiki-admin_modules.php)).

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)

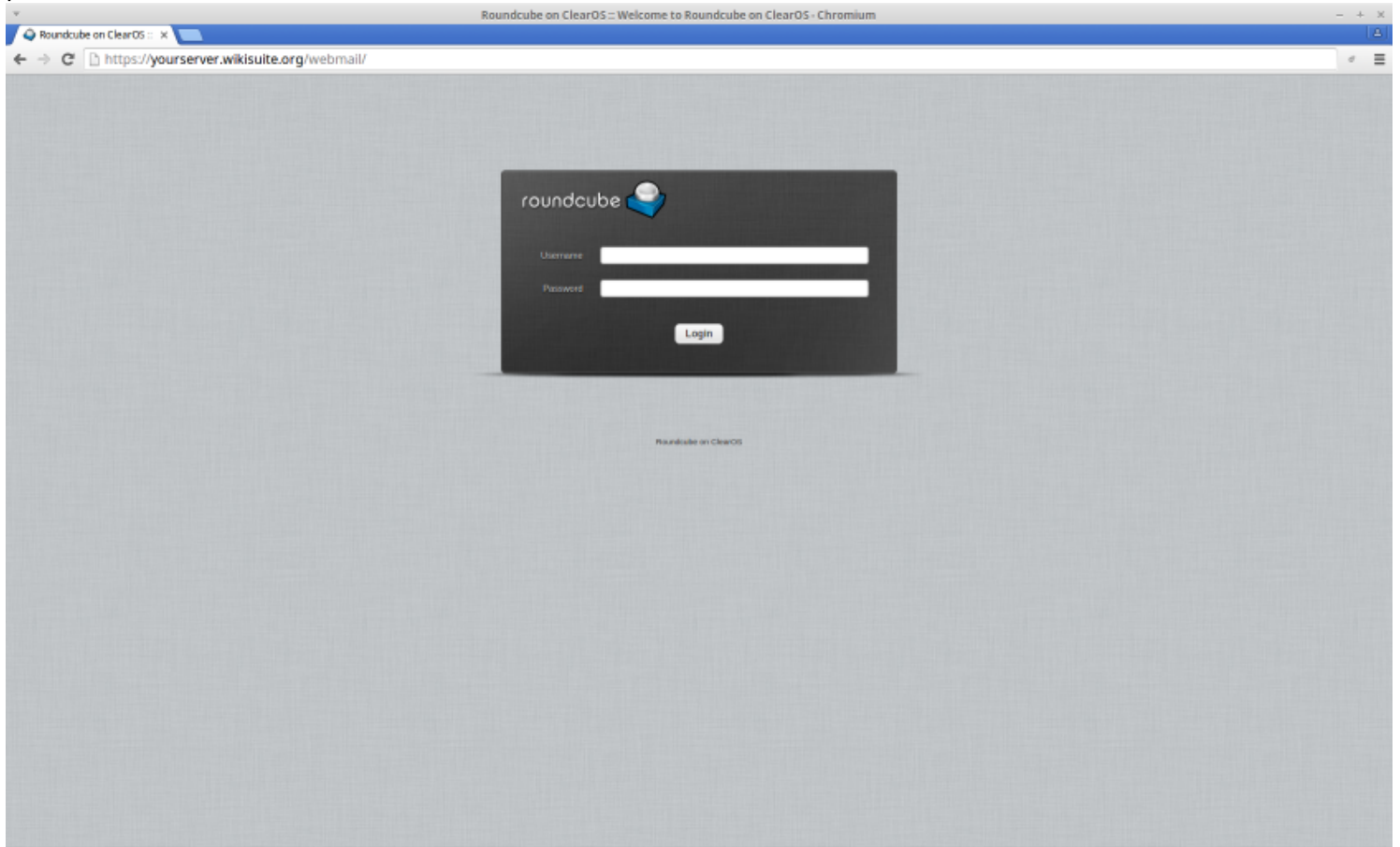
The screenshot shows the Openfire Admin Console interface. The browser address bar displays the URL: <https://wikisuite.net:9091/group-edit.jsp?group=allusers>. The Openfire logo is in the top left, and the user is logged in as 'marc' with a 'Logout' link. The top navigation bar includes 'Server', 'Users/Groups', 'Sessions', 'Group Chat', 'Plugins', 'Fastpath', and 'Meetings'. The 'Users/Groups' section is active, showing a sidebar with 'Users' and 'Groups' tabs. The 'Groups' tab is selected, displaying a list of group management options: 'Group Summary', 'Group Options', 'Edit Group' (highlighted), 'Delete Group', and 'Create New Group'.

The main content area is titled 'Edit Group' and contains the following sections:

- Edit Details:** A message states 'Not allowed: the group account system is read-only.' Below this, the 'Group Name' is set to 'allusers' and the 'Description' is 'All Users'. A red circle highlights the 'allusers' text in the 'Group Name' field.
- Contact List (Roster) Sharing:** A message explains that this feature automatically adds the group to users' contact lists. Two radio buttons are present: 'Disable contact list group sharing' (unselected) and 'Enable contact list group sharing' (selected). A red circle highlights the 'Enable contact list group sharing' option. Below the radio buttons, there is a form to 'Enter contact list group name' with 'allusers' entered, and a 'Share group with:' section with three options: 'Users of the same group' (selected), 'All users' (unselected), and 'The following groups:' (unselected). The 'The following groups:' option has a dropdown menu showing 'guests'.
- A 'Save Contact List Settings' button is at the bottom of the 'Contact List (Roster) Sharing' section.

# Configure email

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

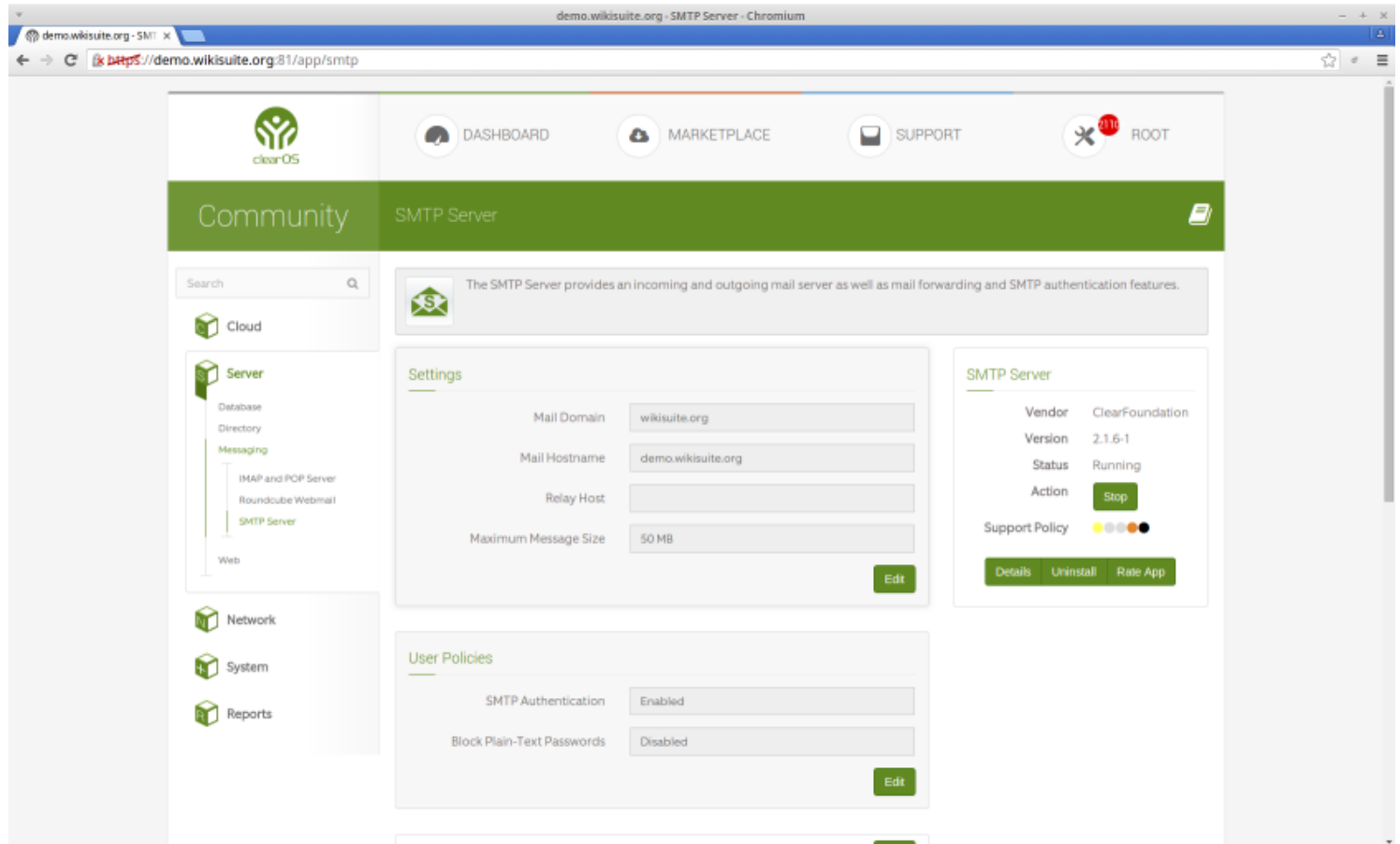


In ClearOS

## Options about sending emails

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

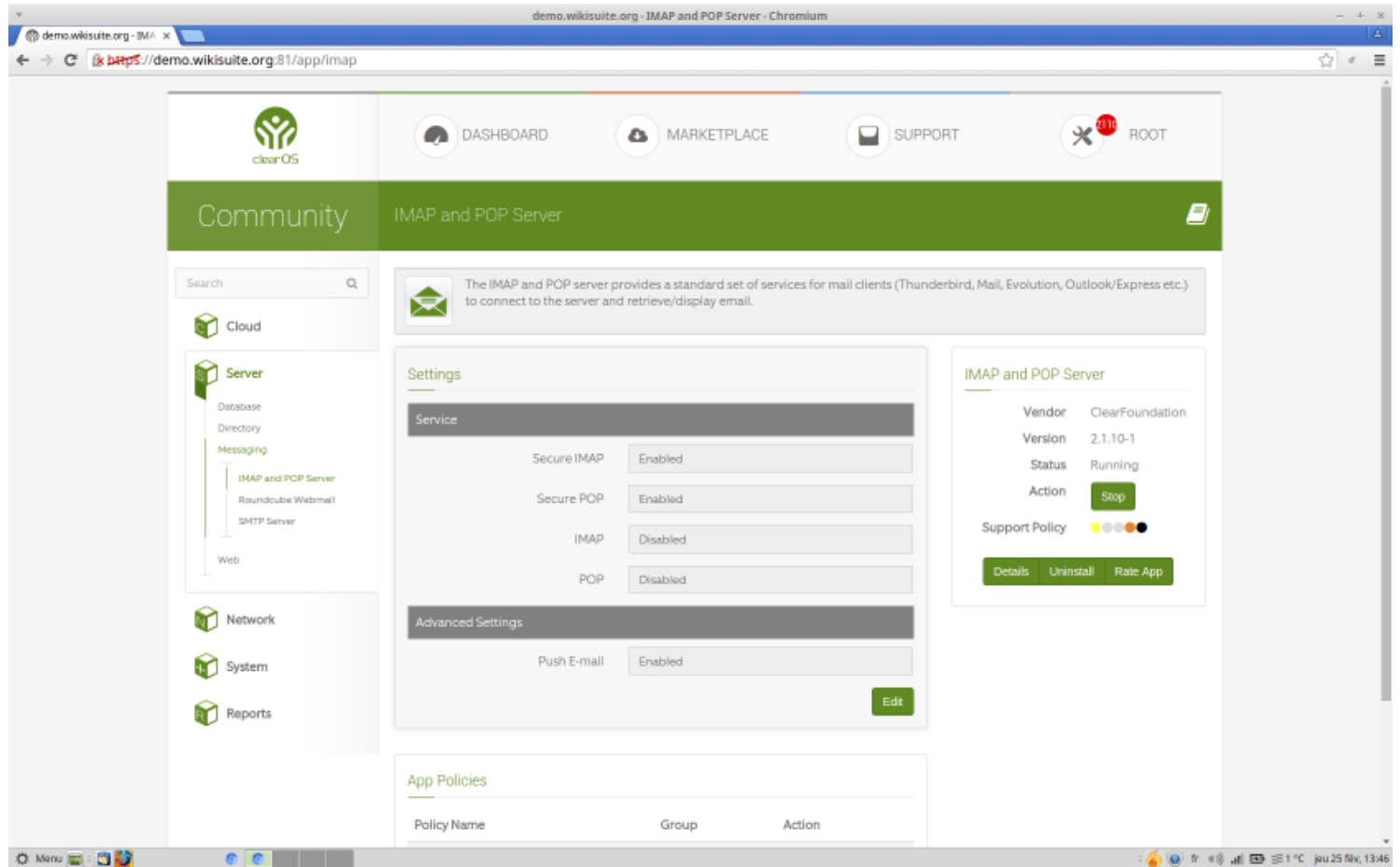
WikiSuite: The most comprehensive and integrated Open Source enterprise solution.



## Options about receiving emails

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

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

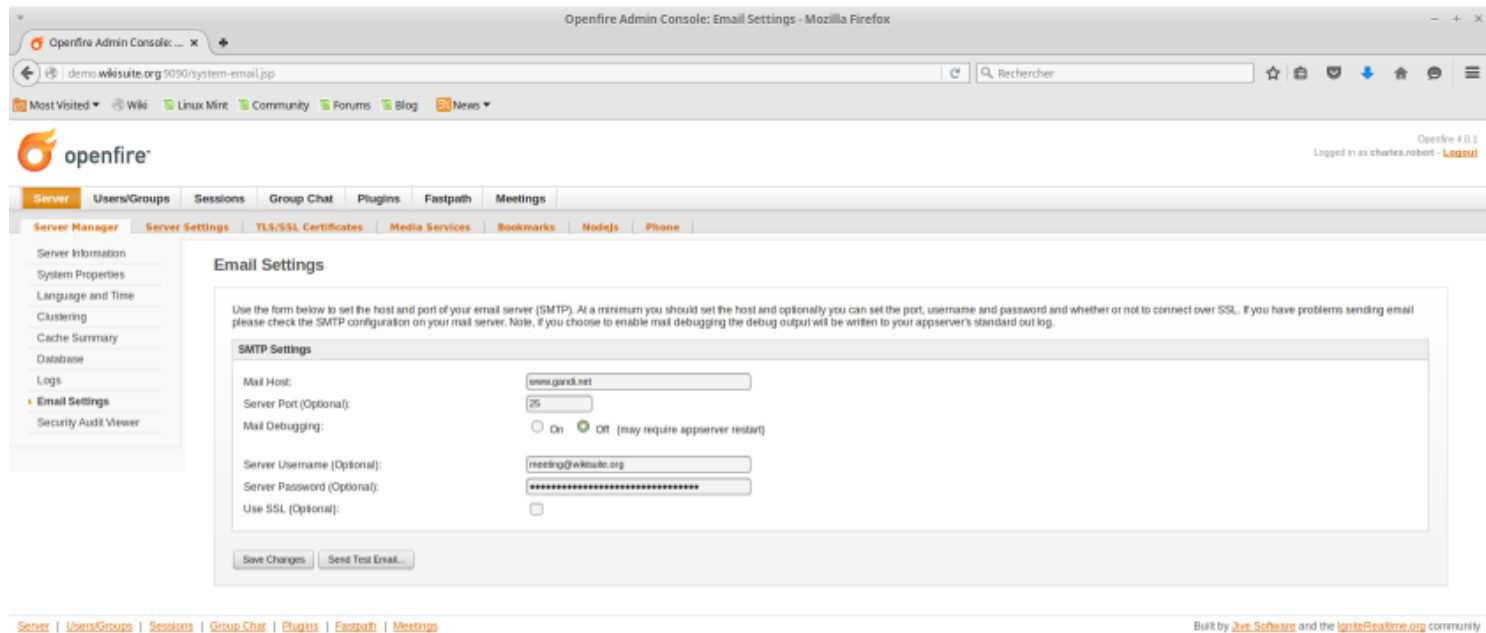


## In Openfire

Edit the email setting in the Server Manager tab as in the image:

<https://example.org:9091/system-email.jsp>

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



Edit the email listener in the Meeting tab as in the image:

<https://example.org:9091/plugins/ofmeet/ofmeet-email-listener.jsp>

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

The screenshot shows the Openfire Admin Console in a Mozilla Firefox browser. The address bar shows the URL: `demo.wikisuite.org:3090/plugins/ofmeet/ofmeet-emailListener.jsp`. The page title is "Openfire Admin Console: Email Listener - Mozilla Firefox". The Openfire logo is in the top left, and the version "Openfire 4.0.1" is in the top right. The user is logged in as "charles.robert". The navigation menu includes: Server, Users/Groups, Sessions, Group Chat, Plugins, Fastpath, and Meetings. The "Meetings" tab is selected, and the "Email Listener" sub-tab is active. The main content area is titled "Email Listener" and contains a form for configuring the email listener service. The form includes fields for Mail Host, Mail Port, Use SSL (Optional), Server Username, Server Password, Folder, and Check Frequency (mills). The values entered are: Mail Host: mail.gard.net, Mail Port: 143, Use SSL (Optional): checked, Server Username: meeting@wikisuite.org, Server Password: [redacted], Folder: Inbox, and Check Frequency (mills): 300000. There are "Save" and "Test Settings" buttons at the bottom of the form. The footer of the page says "Built by Jive Software and the IgniteRealtime.org community".

## 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.

The screenshot shows the Openfire Admin Console interface in a Chromium browser. The address bar displays `demo.wikisuite.org:9090/muc-room-summary.jsp`. The Openfire logo is in the top left, and the version `Openfire 4.0.3` is in the top right, along with the text "Logged in as charles.robert - Logout". The main navigation bar includes `Server`, `Users/Groups`, `Sessions`, `Group Chat` (selected), `Plugins`, `Fastpath`, and `Meetings`. Below this, the `Room Administration` sub-menu is active, showing `Room Summary` and `Create New Room`. The main content area is titled `Group Chat Rooms` and contains a summary: "Below is an overview of the Group Chat Rooms in the service `conference.demo.wikisuite.org`. From here you can view the rooms, edit their properties, and create new rooms. Total Rooms: 3. Sorted by Room ID". A table lists the rooms:

Room	Description	Persistent	Users	Edit	Destroy
1 <code>Team meeting (meet)</code>	Team meeting	<input checked="" type="checkbox"/>	0 / 30		
2 <code>team</code>	team	<input checked="" type="checkbox"/>	1 / 30		
3 <code>Workgroup test Chat Room (workgroup-test)</code>	Workgroup Chat Room	<input checked="" type="checkbox"/>	1 / 0		

The footer of the page states "Built by [Jive Software](#) and the [IgxoftRealtime.org](#) community".

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

The screenshot shows the Openfire Admin Console interface in a Chromium browser. The address bar displays `demo.wikisuite.org:9090/muc-room-edit-form.jsp?create=true`. The Openfire logo is in the top left, and the version `Openfire 4.0.3` is in the top right, along with the text "Logged in as charles.robert - Logout". The main navigation bar is the same as the previous screenshot, with `Group Chat` selected. The `Room Administration` sub-menu is active, and `Create New Room` is selected. The main content area is titled `Create New Room` and contains the instruction: "Use the form below to create a new persistent room. The new room will be immediately available." The form includes the following fields and options:

- Room ID:  @conference.demo.wikisuite.org
- Room Name:
- Description:
- Topic:
- Maximum Room Occupants:
- Broadcast Presence for: ☒ Moderator ☒ Participant ☒ Visitor
- Password Required to Enter:
- Confirm Password:
- Show Real JIDs of Occupants to:

Room Options:

- ☒ List Room in Directory
- ☐ Make Room Moderated
- ☐ Make Room Members-only
- ☐ Allow Occupants to invite Others
- ☐ Allow Occupants to change Subject
- ☐ Only login with registered nickname
- ☒ Allow Occupants to change nicknames
- ☒ Allow Users to register with the room
- ☐ Log Room Conversations

Buttons: `Save Changes` and `Cancel`.

The footer of the page states "Built by [Jive Software](#) and the [IgxoftRealtime.org](#) community".

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

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](http://wiki.xmpp.org/web/Securing_XMPP#Openfire)
- Not like this: .
- 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](#)

## Source code

Source	Packages
<a href="https://github.com/WikiSuite/app-openfire">https://github.com/WikiSuite/app-openfire</a>	<a href="http://koji.clearos.com/koji/packageinfo?packageID=303">http://koji.clearos.com/koji/packageinfo?packageID=303</a>
<a href="https://github.com/WikiSuite/app-openfire-plugin">https://github.com/WikiSuite/app-openfire-plugin</a>	<a href="http://koji.clearos.com/koji/packageinfo?packageID=311">http://koji.clearos.com/koji/packageinfo?packageID=311</a>
<a href="https://github.com/WikiSuite/openfire">https://github.com/WikiSuite/openfire</a>	<a href="http://koji.clearos.com/koji/packageinfo?packageID=302">http://koji.clearos.com/koji/packageinfo?packageID=302</a>

# 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

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

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](#)