# Integrating Axigen with Instant Messaging

## Table of Contents

## 1. Abstract

The present document presents a solution for having a functional Instant Messaging (IM) service integrated with the Axigen mail server and an IM client available from Axigen's Ajax WebMail interface.

The solution includes the Axigen mail server along with a modified version of the Ajax WebMail interface (containing an integrated IM client), a separate free IM server and other free components used for making it functional.

This scenario is mainly intended for use in smaller enterprises and Service Providers that have already implemented the Axigen messaging platform and use it with one or several medium-sized domains. The solution has been fully tested and is recommended by the Axigen Team, but it is NOT officially supported.

## 2. Overview

The IM solution is based on a setup that includes an Axigen mail server with Ajax WebMail service available.

On the client side, a special release of the Axigen Ajax WebMail interface is deployed, having an embedded **Web-based IM Client** that is available for use in the same browser window as the Ajax WebMail interface. The embedded client offers IM features (such as the ability to send and receive instant messages, manage

the user's status and buddy list etc.) and communicates through XMPP (Extensible Messaging and Presence Protocol) over BOSH (Bidirectional-streams Over Synchronous) with an IM service described below.

On the server side, a two-tier setup with the following components will be required:

- at least one **Axigen mail server** that runs with attached Axigen storage in the back-end tier, hosts users' email accounts and provides messaging and collaboration services through the Axigen WebMail interface;
- one **IM Server** that runs in the back-end tier, hosts the users' IM accounts and provides an XMPP-based IM service;
- one **Directory Server** running in the back-end tier, that is used for integration and provides authentication for both email and IM accounts; in case of specific implementations and setup conditions, the directory server may provide LDAP-based account synchronization between the Axigen mail server and IM server on one side, and the LDAP server on the other side;
- at least one stateless **Web Proxy Server** that runs in the front-end tier and dispatches HTTP-based requests in the following way:
  - web pages and SOAP requests coming from the Axigen WebMail interface will be routed to the WebMail service on an Axigen mail server in the back-end tier;
  - XMPP (over BOSH) requests coming from the web-based IM client will be routed to the XMPP service on the IM server.

From the end-user's perspective, things are happening as follows. The user logs in from the login page of the Axigen WebMail interface and, at that moment, a new WebMail session is created based on authentication using the LDAP server through the channel Web Proxy Server - Axigen mail server and a new IM session is created also based on authentication using the LDAP server through the Web Proxy Server - IM Server channel. After a successful authentication, the user simultaneously accesses both the email account and the IM account from the same browser window (tab), being able to work with email messages and folders, PIM information and instant messages at the same time.

In order to have a commonly used degree of security, the WebMail and IM session are usually (and recommended) based on HTTP secure (HTTPS) connections between the browser-hosted components (WebMail interface and IM client) and Web Proxy Server. That is why the Web Proxy Server that is being used should support and provide a HTTPS proxy service.

From the administrator's perspective, there are two possible situations related to user provisioning. If the LDAP Server is used only as a common source of authentication for both WebMail and IM services, then the users' accounts should be provisioned both on the Axigen mail server and the IM Server, and common authentication support should be configured and provisioned in the LDAP Server. If the LDAP Server is also used for synchronizing with the database of accounts on both the Axigen mail server and IM Server, then the users' account should be provisioned only in LDAP, which will be a more convenient and reliable way of managing accounts, since a single point of provisioning may be used.

## 3. Deployment

The proposed IM solution, generally described in the previous section, has been successfully defined, deployed and tested by the Axigen Team, in order to respond to the need of having an IM service available along with the Axigen messaging and collaboration services.

It has been deployed on 32-bit (CentOS 5.4) Linux machines and tested with browsers supported by the Axigen WebMail and it includes the following specific components:

- the component used as Directory Server is the ***OpenLDAP server*** (http://www.openldap.org), version 2.4.21, which is a commonly-used, reliable and easy to integrate free LDAP server;
- the component used as IM Server is the ***eJabberd server*** (http://www.ejabberd.im), version 2.1.5, which is a reliable and scalable XMPP-based free IM server;
- the component used as IM Client embedded in the Axigen WebMail interface is the ***JWChat client*** (http://blog.jwchat.org/jwchat), version 1.0; a modified version, skinned properly for a good graphical integration with the Axigen WebMail interface, is included in a special package of the WebMail HSP files (http://www.axigen.com/mail-server/download/#additional-modules);
- the component used for providing messaging and collaborations services is the ***Axigen mail server***, version 7.6.0;
- the component used as Web Proxy Server is one of the following:
  - the ***Apache Web Server*** (http://httpd.apache.org/) version 2.2.17;
  - the ***Axigen mail server*** version 7.6.1 with the WebMail Proxy service running as a HTTP request dispatcher.

The diagrams below depict the logical components of the solution and the way they have been deployed.

This first diagram shows the solution with the Apache Web Proxy, which can be used if the Axigen License Key does not include the WebMail Proxy Add-on.
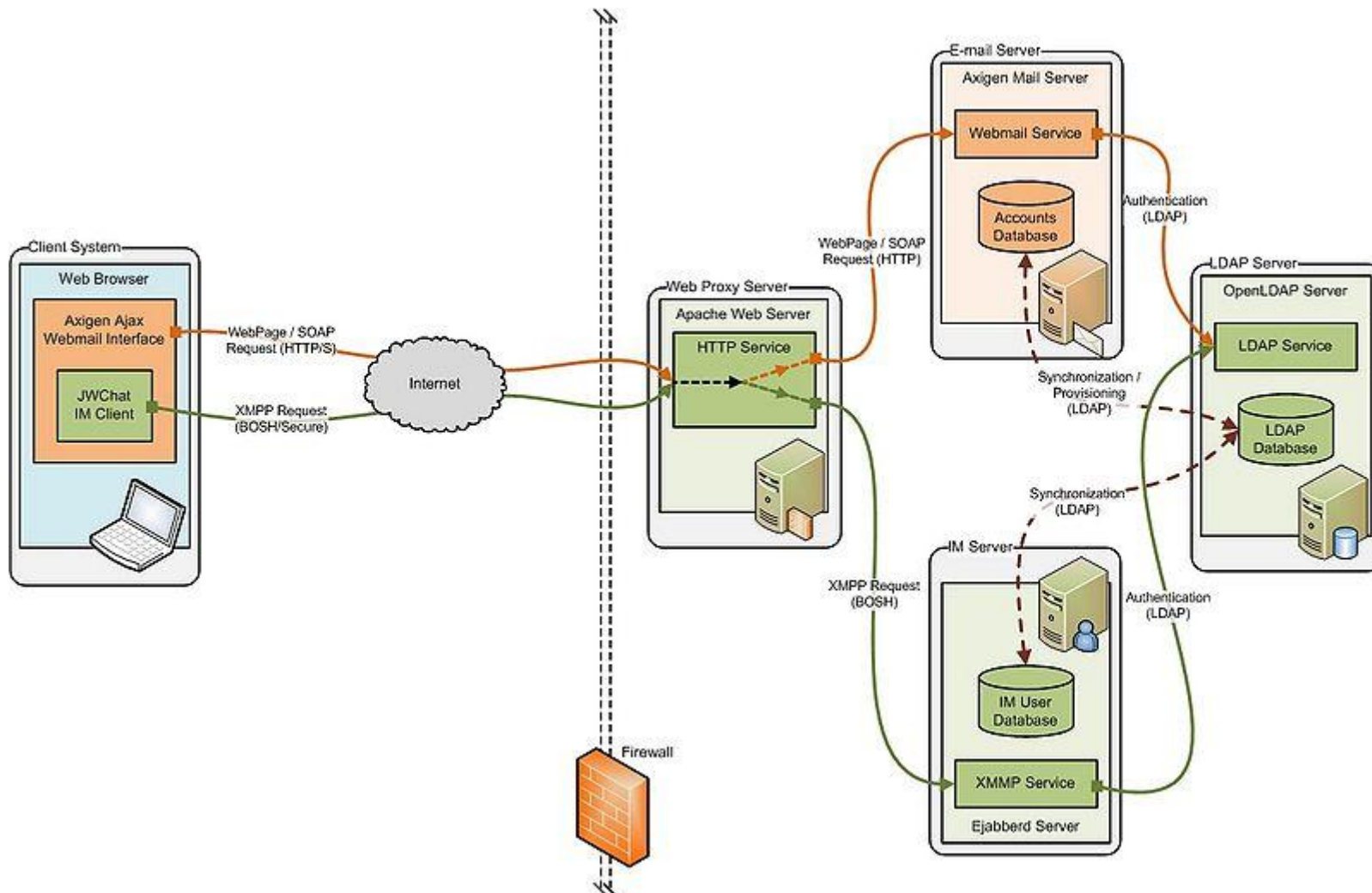
This second diagram shows the solution with the Axigen Web Proxy, which can be used if the WebMail Proxy Add-on is available in the Axigen License Key.
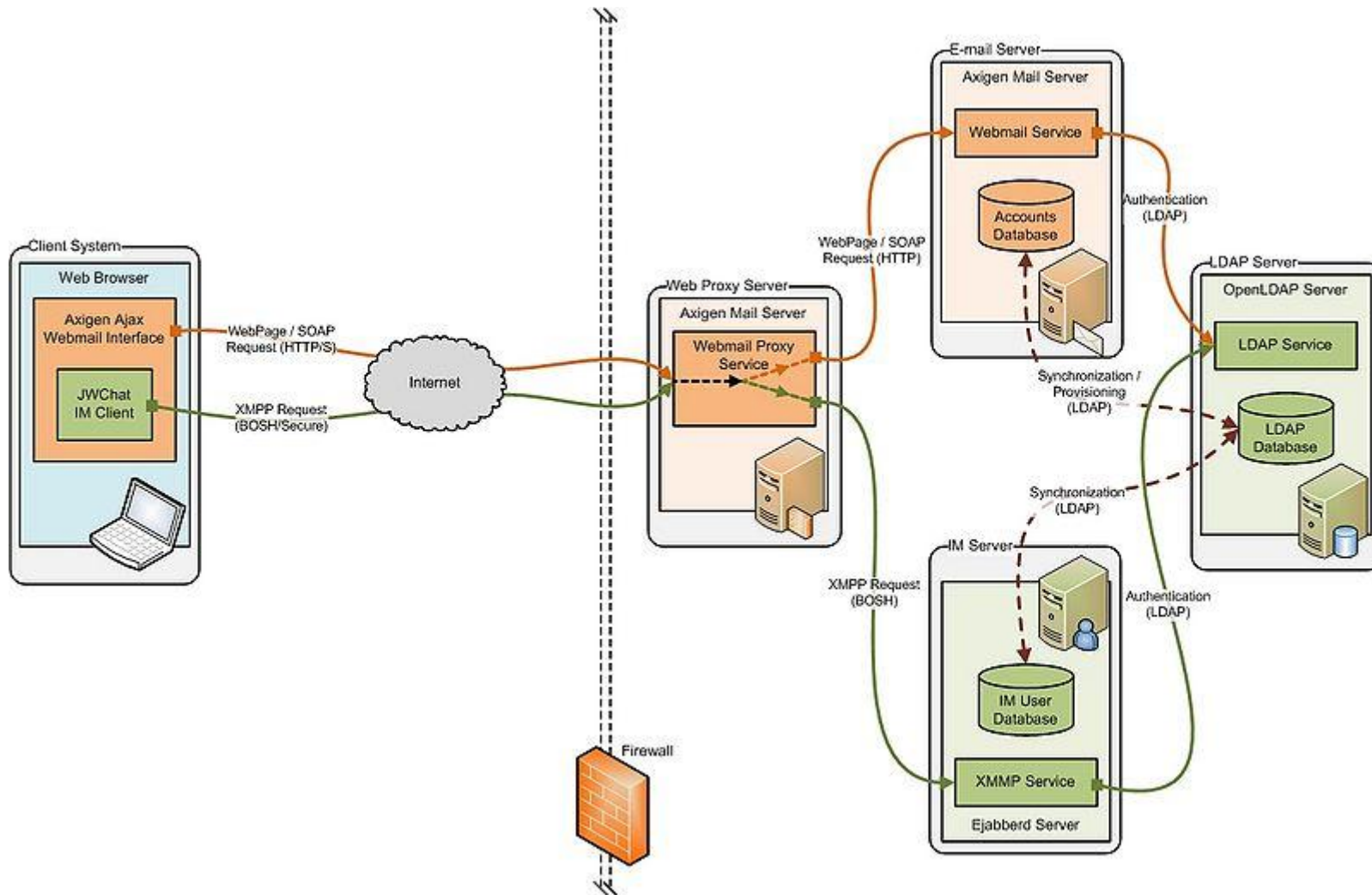
The scenario presented with the proposed solution includes only one domain. Email and IM services will be available to all the accounts in that domain. It is also presumed that the domain is named **"example.org"** for the example purpose. However, the solution is not limited to a single domain, as multiple domains may be deployed in the same setup.

## 3.1 OpenLDAP Server

The OpenLDAP Server must be installed and configured on a Linux host. More information about these operations can be found in the "OpenLDAP Administrator's Guide" available here:
http://www.openldap.org/doc/admin24/

For describing this solution, it is assumed that the OpenLDAP Server runs on a host named **"ldapserver.local"** which should be available in the back-end tier.

The main role of the OpenLDAP server is to support user authentication against the same credentials for both the Axigen mail server and eJabberd IM Server. However, the OpenLDAP server may be configured to support LDAP-based account synchronization with both the Mail and IM servers.

The following configuration settings must be applied to this server in the **"slapd.conf"** configuration file:

- an database and its associated DIT (Directory Information Tree) must be defined; this database will store a LDAP entry for each email account in the **"example.org"** domain hosted on the Axigen mail server and the corresponding IM account hosted on the eJabberd IM Server;
- if account synchronization with the Axigen mail server is going to be used, then the LDAP schema must be extended with the Axigen-specific definitions, and Synchronization Provider must be installed and configured on the OpenLDAP server;
- the defined database will be populated with the root entry corresponding to the **"example.org"** domain and the entry corresponding to the **"postmaster"** account.

With these settings, the **"slapd.conf"** file should include the following information:

```
include          /etc/ldap/schema/core.schema
include          /etc/ldap/schema/cosine.schema
include          /etc/ldap/schema/inetorgperson.schema
include          /etc/ldap/schema/misc.schema

# include Axigen-specific schema definitions
include          /etc/ldap/schema/axigen.schema

pidfile          /var/run/sldapd/slapd.pid
argsfile         /var/run/sldapd/slapd.args
serverID         1

modulepath       /usr/lib/ldap
moduleload       back_bdb.so
moduleload       back_meta.so
moduleload       back_ldap.so

# load sync-provider overlay to support synchronization with Axigen Mail Server
moduleload       syncprov.la

# define database for example.org domain
database         bdb
suffix           "dc=example,dc=org"
rootdn           "cn=admin,dc=example,dc=org"
```

```
rootpw          secret
directory       /var/lib/ldap

index           objectClass                eq
index           ou,cn,mail,surname,givenname    eq,pres,sub
index           entryUUID,entryCSN          eq

# configure sync-provider overlay
overlay              syncprov
syncprov-checkpoint    100 30
syncprov-sessionlog    100
```

More details about this type of synchronization can be found in this article: http://www.axigen.com/knowledgebase/How-to-synchronize-Axigen-to-LDAP_267.html

To populate the LDAP database with the root entry corresponding to the **"example.org"** domain and the entry corresponding to the **"postmaster"** account, the following LDIF files can be used, along with the **"slapadd"** tool:

```
# example.org.ldif file
dn: dc=example,dc=org
objectClass: dcObject
objectClass: organization
dc: example
o: Example Company

dn: cn=Postmaster Account,dc=example,dc=org
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: axiAccount
cn: Postmaster Account
sn: Postmaster
uid: postmaster
userPassword: secret
mail: postmaster@example.org
mobile: +40723445566

slapadd -l example.org.ldif
```

## 3.2 eJabberd IM Server

The eJabberd IM Server must be installed and configured on a Linux host. More information about these operations can be found in the "ejabberd Installation and Operation Guide" available here: http://www.process-one.net/en/ejabberd/guide_en

For describing the solution, it is assumed that the eJabberd IM Server runs on a host named **"imserver.local"** which should be available in the back-end tier.

The role of the eJabberd IM Server is to provide instant messaging capabilities to the users having email accounts on the Axigen mail server. This role is accomplished by responding to the XMPP-over-BOSH request coming from the JWChat IM Client.

In the proposed solution it is important to have some kind of synchronization between the databases of accounts stored in the OpenLDAP Server and for the eJabberd IM Server. Equivalent to such synchronization is to have accounts defined for the eJabberd IM Server stored in the OpenLDAP Server.

Supposing that the Axigen-specific LDAP schema is deployed on the OpenLDAP Server, this is possible by using the special *"mod_vcard_ldap"* module of the eJabberd IM Server and a proper mapping of the LDAP attributes; more information about the usage of this module can be found here: http://www.process-one.net/en/ejabberd/guide_en#htoc64

In order to have groups of IM accounts whose member accounts can see and communicate one with each other, the **shared rosters** capability in the eJabberd IM Server must be enabled.

The following configuration settings must be applied to this server in the *"ejabberd.cfg"* configuration file:

- *"example.org"* must be indicated as being hosted on the IM Server;
- the *"mod_http_bind"* module must be loaded to support the XMPP-over-BOSH protocol;
- a port for receiving XMPP-over-BOSH requests must be opened;
- a secure port for running Axigen's WebAdmin service must be opened; by using this service, an administrator can perform roster management;
- authentication on the IM service must be done in LDAP using *"ldapserver.local"*, so LDAP-based authentication must be configured and enabled;
- administrative permissions must be granted to the *"postmaster"* user from *"example.org"* to allow this user to perform IM service management;
- if LDAP-based account synchronization is going to be used, the *"mod_vcard_ldap"* module must be configured and enabled to store the IM account in the OpenLDAP Server;
- if shared rosters are going to be used, the *"mod_shared_roster"* module must be enabled to support them.

With these settings, the *"ejabberd.cfg"* file should include the following information:

```
%% set example.org domain to be hoster
{hosts, ["example.org"]}.

{listen, [
  %% open the IM service port
  {5280, ejabberd_http, [ http_bind ]}

  %% open WebAdmin service secure port
  {5281, ejabberd_webadmin, [
    web_admin,
    tls,
    {certfile, "/etc/ejabberd/imserver.local.pem"}

  ...
]}.

# set the LDAP-based authentication
{auth_method, ldap}.
{ldap_servers, ["ldapserver.local"]}.
{ldap_encrypt, none}.
{ldap_port, 389}.
{ldap_rootdn, "cn=admin,dc=example,dc=org"}.
{ldap_password, "secret"}.
{ldap_base, "dc=example,dc=org"}.
{ldap_uids, [{"uid", "%u"}]}.

%% grant administrative permissions to postmaster
{acl, admin, {user, "postmaster", "example.org"}}.
{access, configure, {allow, admin}}.

{modules, [
  %% load the module for XMPP-over-BOSH
```

```
    {mod_http_bind, []},

    %% load and configure the module for external LDAP database
    {mod_vcard_ldap, [
      {ldap_servers, ["mydomainhost"]},
      {ldap_rootdn, "cn=admin,dc=mydomain,dc=test"},
      {ldap_password, "secret"},
      {ldap_base, "dc=mydomain,dc=test"},
      {ldap_vcard_map, [
        {"NICKNAME", "%s", ["axiNickName"]},
        {"FN", "%s", ["displayName"]},
        {"FAMILY", "%s", ["sn"]},
        {"GIVEN", "%s", ["givenName"]},
        {"MIDDLE", "%s", ["axiMiddleName"]},
        {"ORGNAME", "%s", ["axiCompany"]},
        {"ORGUNIT", "%s", ["axiDepartment"]},
        {"CTRY", "%s", ["c"]},
        {"LOCALITY", "%s", ["l"]},
        {"STREET", "%s", ["street"]},
        {"REGION", "%s", ["st"]},
        {"PCODE", "%s", ["postalCode"]},
        {"TITLE", "%s", ["title"]},
        {"URL", "%s", ["wWWHomePage"]},
        {"TEL", "%s", ["mobile"]},
        {"EMAIL", "%s", ["axiPersonalEmail"]},
        {"BDAY", "%s", ["axiBirthday"]},
        {"ROLE", "%s", ["axiProfession"]} ]},
      {ldap_search_fields, [
        {"User", "%u"},
        {"Nickname", "axiNickName"},
        {"Given Name", "givenName"},
        {"Family Name", "sn"},
        {"Email", "axiPersonalEmail"} ]},
      {ldap_search_reported, [
        {"Full Name", "FN"},
        {"Given Name", "GIVEN"},
        {"Family Name", "FAMILY"},
        {"Email", "EMAIL"} ]} ]}

    %% load the module for shared rosters
    {mod_shared_roster, []},

    ...
]}.
```

## 3.3 Axigen Mail Server

The Axigen mail server must be installed and configured on a Linux host. More information about these operations can be found in the Axigen mail server documentation available here:
http://www.axigen.com/mail-server/documentation.php

For describing the solution, it is supposed that the Axigen mail server runs on a host named *"mailserver.local"* which should be available in the back-end tier.

The role of the Axigen mail server is to provide email-based messaging and collaboration capabilities to the users having email accounts on the Axigen mail server. This role is mainly accomplished by the Axigen WebMail interface loaded in a web browser and the WebMail service running server-side.

The following configuration settings must be applied to this server by using the administration services (WebAdmin or CLI) or the **"axigen.cfg"** server configuration file:

- the WebMail service must be enabled;
- standard listener must be defined and enabled for this service, with no SSL support;
- a special version of WebMail HSP files (http://www.axigen.com/mail-server/download/#additional-modules) with an embedded JWChat IM Client must be installed in a location (**"webmail-im/"**) that is used as page source directory by the WebMail service;
- authentication on the WebMail service must be done in LDAP by using **"ldapserver.local"**, so a LDAP connector for this server must be defined and used;
- the **"example.org"** domain must be created using administrative services;
- if LDAP synchronization is going to be used, the same LDAP connector must be used for the synchronization of accounts in the **"example.org"** domain.

With these settings, the **"axigen.cfg"** file should include the following information:

```
Server {
  serverName = "mailserver.local"

  # enable Webmail service
  services = (
    webmail
    ...
  )

  userDb = {
    # define a LDAP connector used for authentication and possibly for
synchronization
    ldapConnectors = (
      {
        name = "ldapserver"
        ldapURI1 = "ldap://ldapserver.local:389"
        serverType = OpenLDAP
        bindDN = "cn=admin,dc=example,dc=org"
        bindPass = "secret"
        synchronizationDirection = bothWays
        synchronizationConflictResolution = ldapWins
        accountBaseDN = "dc=example,dc=org"
        ...
      }
      ...
    )
    ...
  }

  webmail = {
    # enable default listener for Webmail service
    listeners = (
      {
        address = "0.0.0.0:8000"
        enable = yes
        sslEnable = no
        ...
      }
      ...
    )

    # set HSP source location to pages including IM support
    path = "webmail-im/"
```
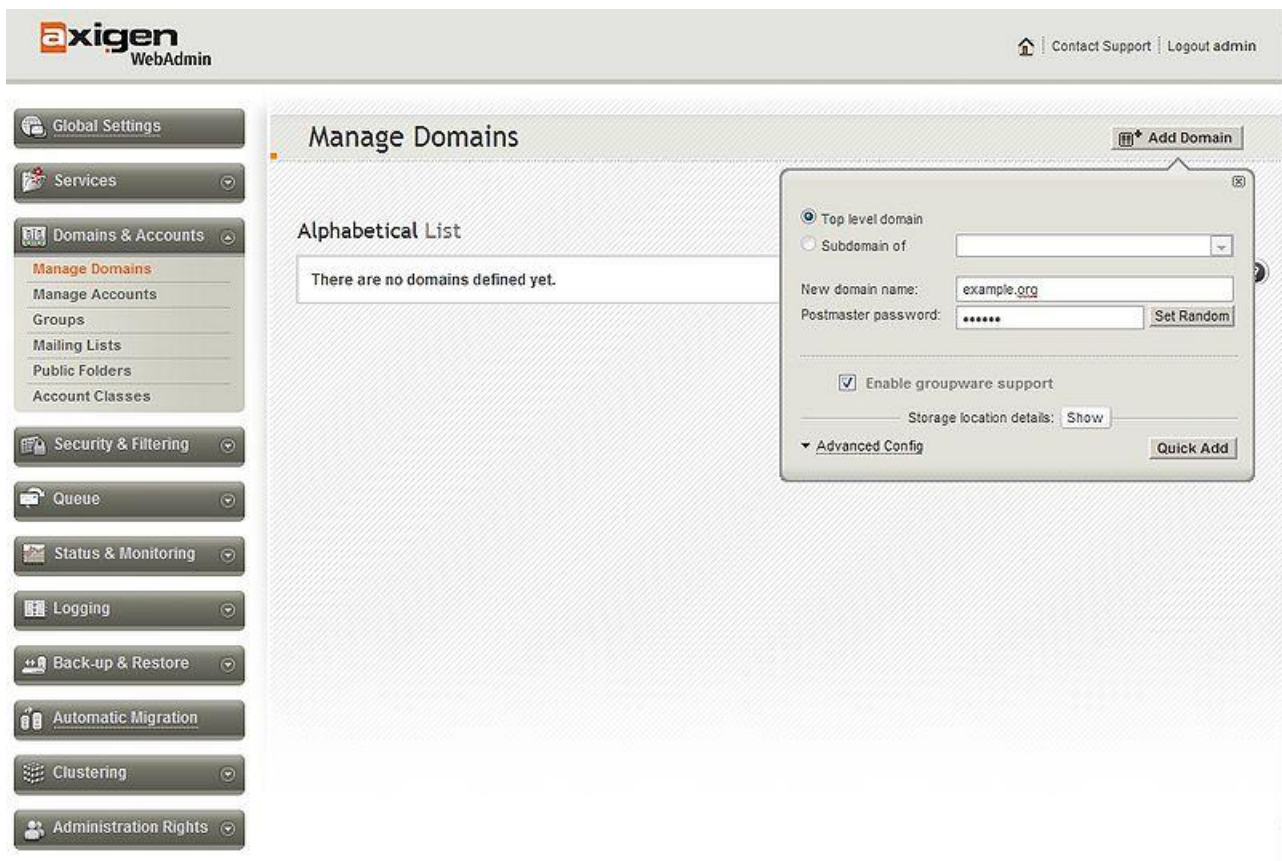
```
    # set LDAP-based authentication through the defined connector
    userDbConnectorType = ldapBind
    userDbConnectorName = "ldapserver"

    ...
  }


  ...
}
```
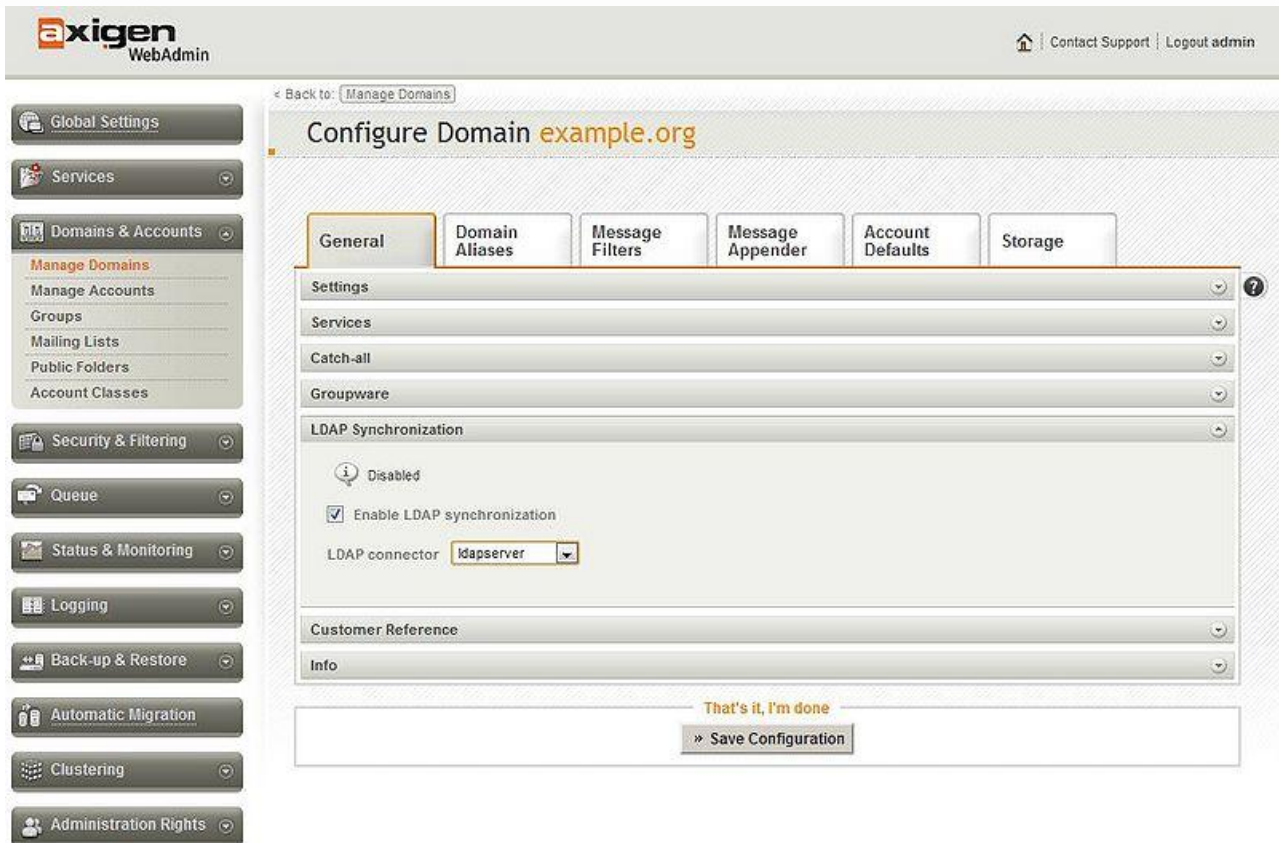
The **"example.org"** domain can be created by using the WebAdmin service, from the **"Manage Domains"** page:



The LDAP synchronization can also be enabled on the **"example.org"** domain from the WebAdmin service, from the **"Configure Domain"** page:

## 3.4 Apache Web-Proxy

The Apache Web Server must be installed and configured on a Linux host. More information about these operations can be found in the "Apache HTTP Server Documentation available here: http://httpd.apache.org/docs/2.0/

For describing the solution, it is assumed that the Apache Web Server runs on a host named **"webmail.example.org"** which should be available in the front-end tier and should be visible from the Internet.

The role of the Apache Web-Proxy is to separate and dispatch the WebMail request coming from the Axigen WebMail interface to the Axigen mail server in the back-end tier, and the XMPP-over-BOSH requests coming from the JWChat IM Client to the eJabberd IM Server also running in the back-end tier.

The **"mod_proxy"** module is used to implement the dispatching of the requests. The following configuration settings must be applied to this server and they are reflected in the content of the **"httpd.conf"** configuration file:

- a virtual host must be defined, listening on the 443 secure port;
- SSL server certificate must be generated and deployed on the server;
- rules must be defined for dispatching the HTTP requests separately, depending on their initiator: the WebMail interface or the IM client.

With these settings, the **"httpd.conf"** file should include the following information:

```
<VirtualHost *:443>
    ServerName webmail.example.org
    LogLevel warn
    ErrorLog /var/log/apache2/jwchat_error
```

```
    CustomLog /var/log/apache2/jwchat_access combined

    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on
    SSLProxyEngine on

    #  SSL Certificate
    SSLCertificateFile    /etc/ssl/certs/webmail.example.org.pem
    SSLCertificateKeyFile /etc/ssl/private/webmail.example.org.key

    # Route http-bind requests to IM Server
    ProxyPass /http-bind/ http://imserver.local:5280/http-bind/
    ProxyPassReverse /http-bind/ http://imserver.local:5280/http-bind/

    # Route all other requests to Email Server
    ProxyPass / http://mailserver.local:80/
    ProxyPassReverse / http://mailserver.local:80/

    AddDefaultCharset UTF-8
    Options +MultiViews
</VirtualHost>
```

## 3.5 Axigen Web-Proxy

The Axigen mail server must be installed and configured with the WebMail-Proxy service active. The capability of separating the Axigen WebMail requests from BOSH requests and dispatching the former ones to an Axigen mail server in the back-end, and the later ones to an eJabberd IM Server, is going to be available in Axigen version 7.6.1. This capability is provided by the WebMail-Proxy service running in a restricted mode, in which the other functions of this service (e.g. routing and authentication) are not available.

For describing the solution, it is assumed that the Axigen mail server with Web-Proxy role runs on a host named **"webmail.example.org"** which should be available in the front-end tier and should be visible from the Internet.

The following configuration settings must be applied to this server by using the administration services (WebAdmin or CLI) or the **"axigen.cfg"** server configuration file:

- the WebMail-Proxy service must be enabled, if it is available from the License Key;
- a secure listener must be defined and enabled for this service, with no SSL support;
- the SSL server certificate must be generated and deployed on the server;
- define rule for static forwarding of HTTP requests coming from the WebMail interface;
- define rule for static forwarding of XMPP-over-BOSH requests coming from the IM client.

With these settings, the **"axigen.cfg"** file should include the following information:

```
Server {
  # enable Webmail-Proxy service
  services = (
    ...
    webmailProxy
    ...
  )
  ...
  webmailProxy = {
```

```
# enable a secure listener
listeners = (
  {
    address = "193.230.245.1:443"
    enable = true
    sslEnable = yes
    sslControl = {
        certFile = "webmail.example.org.pem"
        ...
    }
  }
)
# static routing of the requests coming from Webmail interface
mappingData = {
  userMap = "none"
  mappingHost = "mailserver.local"
  mappingPort = "8000"
}
# NEWLY INTRODUCED: static routing of the requests coming from IM client
httpBindBackend = "http://imserver.local:5280"
  ...
  }
  ...
}
```

## 3.6 JWChat IM Client

The JWChat IM Client is a free open-source web-based IM client, developed using Ajax technology and using XMPP-over-BOSH to communicate with an IM server having such support, such as the case with the eJabberd IM Server. The client has been skinned in order to have a proper graphical integration with the Axigen WebMail interface. The modified source code has been inserted into the package of the Axigen WebMail HSP files.

Considering that the special package including IM support is installed in the **"webmail-im/"** directory of the **"mailserver.local"** host, the JWChat files are installed under the sub-directory **"webmail-im/jwchat/".**

The IM support must be enabled in order to be available (loaded) within the Axigen WebMail interface. This can be done by using the following setting in the **"webmail-im/private/index.hsp"** page:

```
<% IM_SUPPORT = "true" %>
```

The JWChat IM Client must be instructed where to send its requests. This can be done by using the following configuration settings that must be inserted into the "**webmail-im/jwchat/config.js"** file:

```
// use secure connection
var CONNECTION_SECURE = true;
// set the address for the destination server
var IM_SERVER_URL = "https://webmail.example.org:443/http-bind/";
```

If secure communication is set, then the CA certificate must be added to the trusted CA certificates in the browser being used and, also, the SSL server certificate must be added to the trusted sites certificates in the same browser. If the CA certificate is not added to the browser CA certificate list, the user has to manually add a server certificate exception for the **"webmail.example.org"** server.

# 4. Usage

## 4.1 Starting Services

After installing and configuring all the servers in the way indicated in the previous section, the services on these servers must be started in a certain order.

The LDAP service on the OpenLDAP Server must be started first, to be available for authentication and possibly synchronization with the Axigen mail server and eJabberd IM Server. This can be done with the following command run as *"root"* user on the **"ldapserver.local"** host:

```
/etc/init.d/slapd start
```

The IM service on the eJabberd IM Server must be started, using the following command run as *"root"* user on the *"imserver.local"* host:

```
/etc/init.d/ejabberd start
```

The messaging services on the Axigen mail server must be started, using the following command run as *"root"* or *"axigen"* user on the *"mailserver.local"* host:

```
/etc/init.d/axigen start
```

The web-proxy service on the Apache Web-Proxy Server must be started, using the following command run as *"root"* user on the *"webmail.example.org"* host:

```
/etc/init.d/httpd start
```

If the Axigen Web-Proxy Server is used, the web-proxy service must be started in way similar to the one for the Axigen mail server.

## 4.2 Account Provisioning

Account provisioning includes the following three operations: create account, update account settings and delete account, applied for both email and IM accounts.

If only LDAP-based authentication is used in the proposed IM solution, the account provisioning must be performed in three points: on the OpenLDAP server (at least account credentials), on the Axigen mail server and on the eJabberd IM Server.

However, the more convenient way for the proposed IM solution is to used LDAP-based synchronization between the Axigen mail server and OpenLDAP Server and the synchronization-equivalent functionality of deploying the IM accounts for the eJabberd IM Server in the same OpenLDAP Server. In this case, the major advantage is having a *single point of account provisioning* only on the OpenLDAP server.

To populate the directory with information about your organization, create a **ldif** file: Simultaneously, an email account and an IM account are created by adding a proper entry in LDAP database, by using a LDIF file like the following one, along the *"ldapadd"* tool:

```
# john.doe-example.org.ldif
dn: cn=John Doe,dc=example,dc=org
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

```
objectClass: axiAccount
cn: John Doe
sn: Doe
givenName: John
uid: john.doe
userPassword: qwe123
mail: john.doe@example.org
mobile: +40723555666
axiNickName: Johnny
axiCompany: Example Company
axiDepartment: Sales
axiPosition: Account Manager

ldapadd -D "cn=admin,dc=example,dc=org" -W -x -f john.doe-example.org.ldif
```

In case the LDAP synchronization between the Axigen mail server and OpenLDAP Server is set to the **"bothWays"** mode (meaning that any change in the OpenLDAP Server will be propagated to the Axigen mail server and the other way around), then an additional single point of account provisioning may be considered on the Axigen mail server through its administrative (CLI and WebAdmin) services.
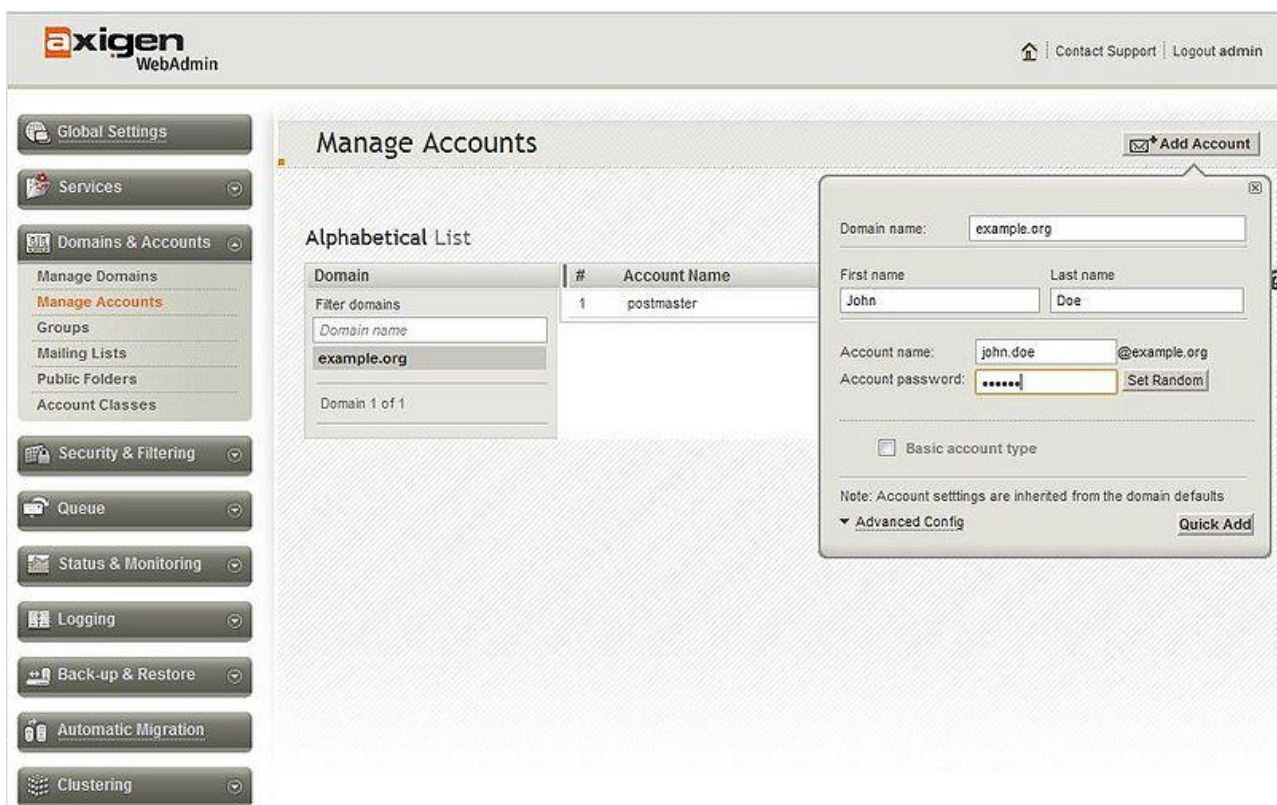


## 4.3 Roster Management

Shared rosters can be defined through the eJabberd WebAdmin interface which, in the presented scenario, can be accessed by using the URL "*https://imserver.local:5281/admin*" and the **"postmaster@example.org"** account. To create only a group with all the accounts in the **"example.org"** domain, one shared roster **@all@** with all IM accounts may be created.

Multiple rosters in the same **"example.org"** domain can be defined by using the same interface, each one possibly corresponding to a department within the organization that owns this domain.
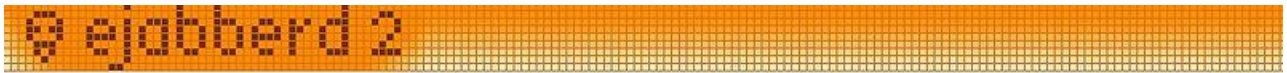
Member-account can be added for each defined roster, also by using the eJabberd WebAdmin interface.



More details about shared roster can be found here:
http://www.process-one.net/en/ejabberd/guide_en#htoc59.

## 4.4 Email and IM Services

The Instant Messaging service can be accessed by the users directly from Axigen's Ajax WebMail. The list of available contacts, grouped in rosters, is integrated on the right side of the interface.
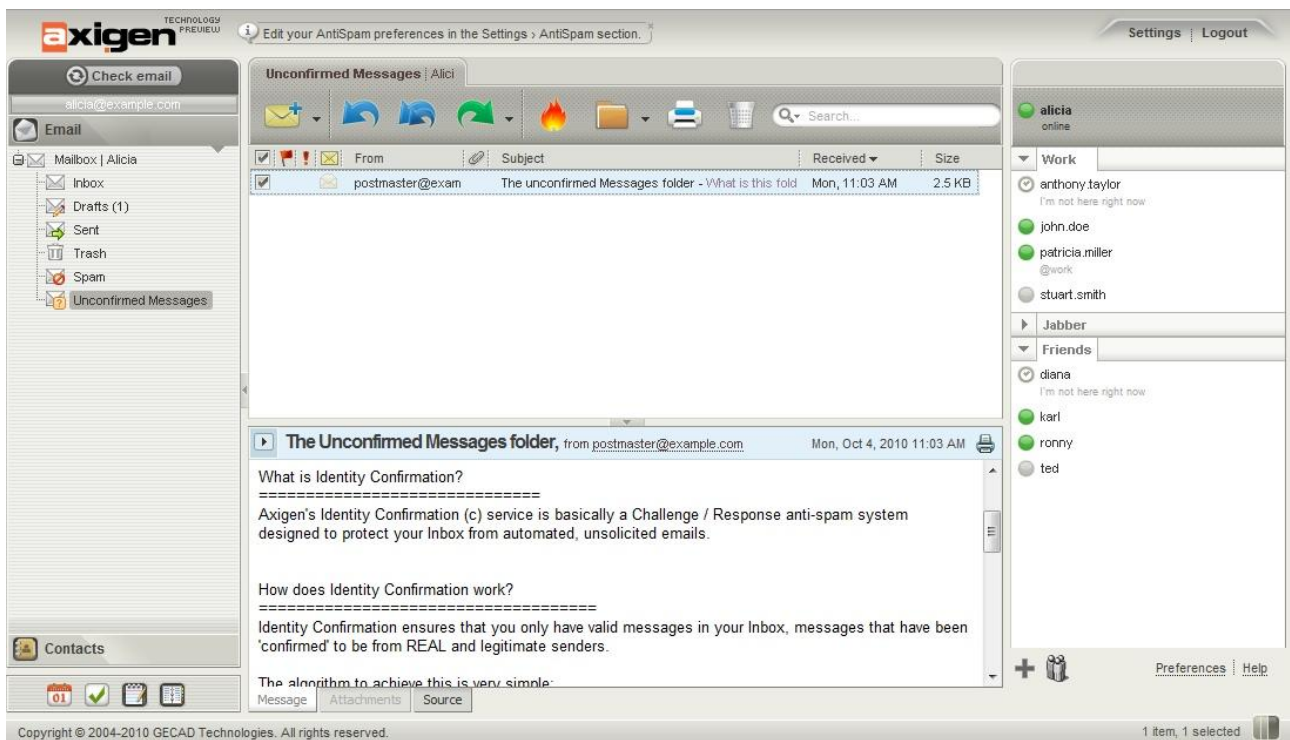


The user can see his / her username and status at the top of the list of users. Clicking on the status icon (indicator) allows the user to change his / her status, by choosing a new one from the list, as well as set a custom status message. Here are the possible statuses, along with their associated icons (indicators):

- User is online / User is willing to chat
- User is away
- User is not available / User doesn't want to be disturbed
- User is offline / User is invisible
- User hasn't authenticated you
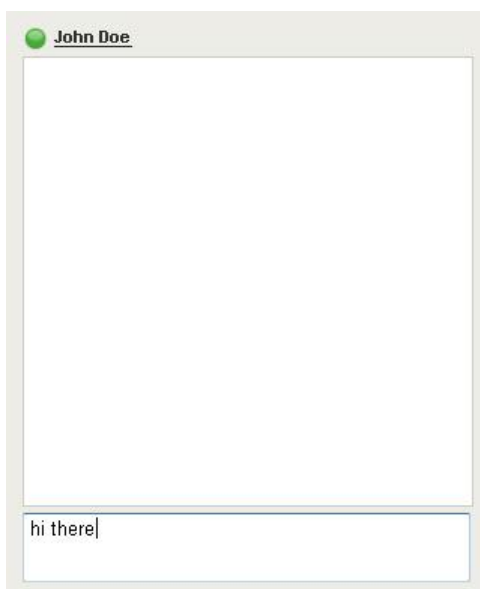


Left-clicking on a user pops up a message window.
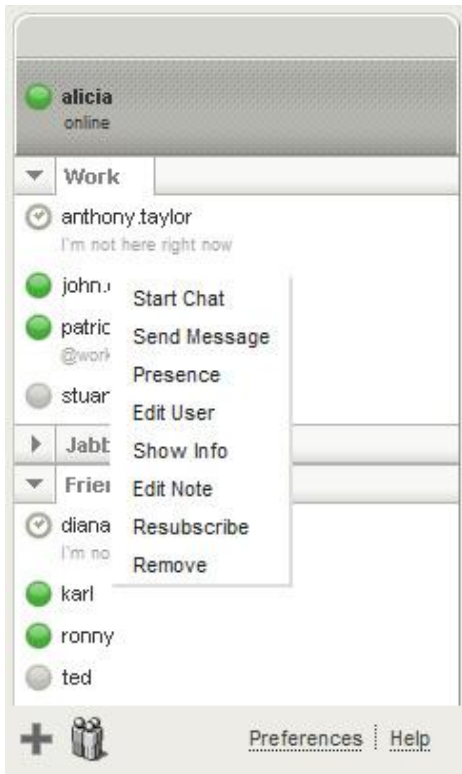
A set of operations can be performed when right-clicking on a user in the list, by simply using the contextual menu. Common options include:

- Send Message: Opens the message dialog for this user.
- Start Chat: Opens a chat window for this user.
- Edit User: Opens the edit dialog for this user, where his nickname can be set and the groups he / she belongs to can be changed.
- Show Info: Shows the user's profile.
- Resubscribe: Opens a subscription request for this user
- Remove: Removes this user from the contact list (completely) and revokes the authentication for him / her (if any).

New users can be added by clicking on the **"+"** icon below the contact list.

The **"Preferences"** window allows users to customize their IM client (e.g. have offline users shown or hidden, play sounds) and can be opened by clicking on the corresponding link below the contact list.

## 5. Conclusions

The proposed IM solution is mainly addressed to small enterprises and Service Providers and can scale up to 1000 users within tens of domains. The scenario presented here includes a single domain corresponding to a single organization. In a scenario for Hosting Providers, multiple domains corresponding to different organizations or organizational units can be defined by making the proper configuration extensions for the OpenLDAP Server, eJabberd IM Server and Axigen mail server.

The setup presented in this document included only one host for each type of server: LDAP Server, Email Server, IM Server and Web-Proxy. To scale up to a much larger number of accounts, Axigen's plans for future developments of this solution include supporting multiple Axigen Web-Proxies with dynamic LDAP-based routing of requests towards multiple Axigen mail servers and eJabberd IM Servers running in the back-end tier.

The proposed solution has been tested on hosts with 32bit CentOS 5.5 Linux. The Axigen mail server and Axigen Web-Proxy can run on 64bit Linux platforms or on 32bit and 64bit Windows platforms. The Apache Web-Proxy and eJabberd IM Server can run on 64bit Linux platforms or 43bit Windows platforms.

Other Axigen plans include:
- configurable availability and functionality of the IM service in Axigen WebMail interface; this kind of configuration should be available from the Axigen administration services (CLI and WebAdmin);
- more features available in the IM client (e.g. file transfer) and a better integration of the IM client with the Axigen WebMail interface;
- an enhanced management of the IM buddy list in direct relationship with the user's contact lists.
- a better integration of the roster management on the eJabberd Server better with the Axigen mail server and OpenLDAP Server.