TripLOA
Security Module

Documentation

Francesco Fontana < francesco.fontana@gmail.com >
Ugo Moschini < ugomoschini@yahoo.it >
Marco Sparagna < marco.sparagna@gmail.com >
Daniele Vitale < vitaled@gmail.com >

Table of contents

The .NET Membership Framework

The techniques used in TripLOA for authenticating visitors, authorizing access to particular pages and functionalities rely on the ASP.NET Membership Framework.
This framework is a handful of classes in the System.Web.Security namespace that provide functionalities for performing essential user account related tasks, from the registration of a new user to administrative tasks.

The main goals of this module of TripLOA are:

- Identify and log users into TripLOA ;
- Use ASP.NET's Membership framework to manage user accounts ;
- Create, update, and delete user accounts ;
- Limit access to a web page, directory, or specific functionality based on the logged in user ;
- Use ASP.NET's Roles framework to associate user accounts with roles ;
- Manage user roles ;
- Limit access to a web page, directory, or specific functionality based on the logged in user's role ;
- Use, customize and extend ASP.NET's security Web controls

An introduction and useful tutorials can be found at www.asp.net/learn/security.

The Membership Provider class "SqlMembershipProvider" shipped by Microsoft has been used. It implements the Membership API with a SQL Server database. The same for the "SqlRoleProvider" class.

Configuring the Membership Framework

Three files are present in the folder /WebConfigs. They are the web.config files for TripLOA application, according to the kind of build you want (for example, local or remote access to the Sql database).

The Membership Provider can be easily tuned and configured modifying the tags of the web.config file.

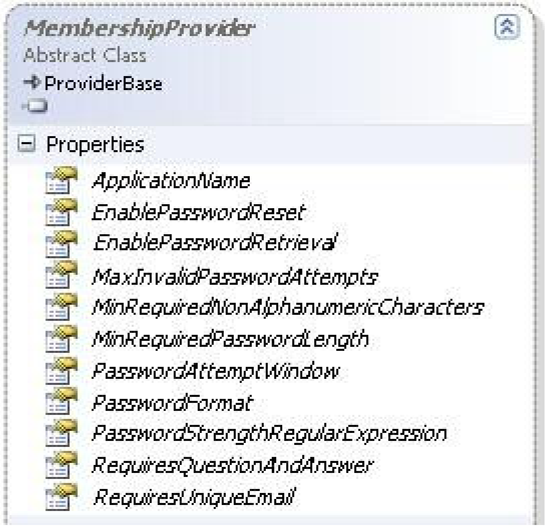
Locate a SqlServer

You can configure how SqlMembership provider interacts with SqlServer.
The connectionStrings tag contains the connection string for the database you want to use for your Membership Provider. Below an example in the case of local database.

```
<connectionStrings>
<add name=
      "Storage.Properties.Settings.LocalTripLoaDbConnectionString"

      connectionString="DataSource=localhost\sqlexpress;InitialCatalog=
      Triploadb;Integrated Security=true;MultipleActiveResultSets=true"

      providerName="System.Data.SqlClient" />
</connectionStrings>
```

Configuring the Membership Provider

The Membership Provider properties that can be modified through Web.Config file are:



MembershipProvider
Abstract Class
→ ProviderBase

Properties
- ApplicationName
- EnablePasswordReset
- EnablePasswordRetrieval
- MaxInvalidPasswordAttempts
- MinRequiredNonAlphanumericCharacters
- MinRequiredPasswordLength
- PasswordAttemptWindow
- PasswordFormat
- PasswordStrengthRegularExpression
- RequiresQuestionAndAnswer
- RequiresUniqueEmail

The passwordFormat property specifies how the provider will store passwords, and will impact a number of other membership features. The SqlMembershipProvider supports three formats: hashed, encrypted and clear.
The provider is set to ‘hashed’ by default. The hashed format passes a user’s plaintext password and a random salt value through a one-way hash algorithm before storing the password. You cannot retrieve a hashed password. To validate a password, the provider has to salt and hash the entered password and compare the two hash .

The enablePasswordRetrieval tag determines if the provider will return a user’s password with the GetPassword method. It is set to true. If the password format is set to ‘hashed’, as in TripLOA, passwords are not retrievable. In the event of a lost password the provider reset the user’s password to a new value and email the new password. In order to do this the framework requires that requiresUniqueEmail property is set to true.

The enablePasswordReset property is set to true by default. It controls the ResetPassword API. ResetPassword will assign a new, generated password to a user. The PasswordRecovery control can automatically email the new password to a user. In the web.config file, there is an area in the ‘mailsettings’ tag used to set an SMTP configuration.

RequiresQuestionAndAnswer property is set to true to prevent a malicious user from resetting someone else's password, A value of true means the user has to provide the answer to a security question before resetting their password. The question and answer text is will be required by the Registration form when registering a new user.

A number of properties control the password strength a provider will allow. The minRequiredPasswordLength has been set to 4 characters and minRequiredNonalphanumericCharacters to 0 in order to perform the debug phase in ease. These properties can be easily modified with the desired value.

The maxInvalidPasswordAttempts and passwordAttemptWindow properties work together to prevent a malicious user from using brute force techniques to break into a user account. Too many bad passwords will lock out a user account and prevent the account from logging in until the account is unlocked with the UnlockUser method. This policy can be tuned easily by settings the desired value of maxInvalidPasswordAttempts and passwordAttemptWindow.

Configuring the Role Provider

The role provider allows you to create roles and map users into the roles. TripLOA has two roles: Administrators and Members. Given a username, the role manager can tell you to which roles a user belongs. Areas of TripLOA, or specific operations, can be restricted to exact roles.
In the Web.Config file, you simply determine if you want to use a Role Provider:

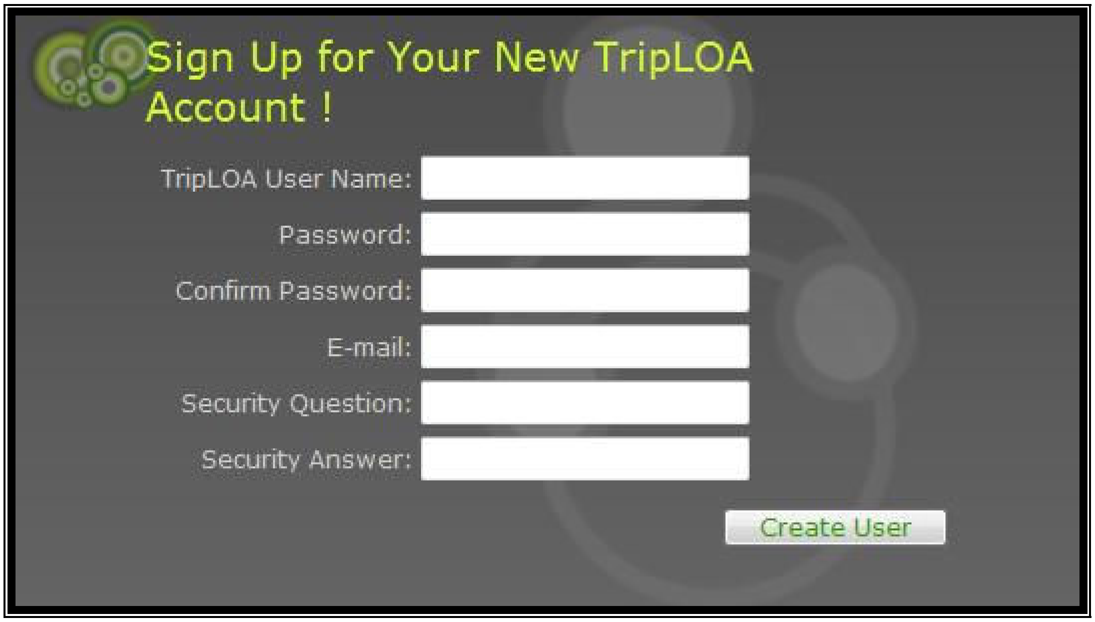
```
 <roleManager enabled="true" defaultProvider="SecuritySQLRoleProvider">
      <providers>
      <add name="SecuritySQLRoleProvider"

      type="System.Web.Security.SqlRoleProvider"

      connectionStringName="Storage.Properties.Settings.LocalTripLoaDbC
      onnectionString"/>
      </providers>
    </roleManager>
```

Creating or deleting roles or assigning roles to existing users can be easily done in the TripLOA administration pages.

The user's pages

Register a new user

Mainly, a visitor can register to TripLOA through the page /Registration.aspx.
This page contains a simple WebControl, managing the process of registration. The registration procedure assigns transparently a role (the 'Members' one) to the new user, in order to display the correct functionalities according to its precise role during the usage of TripLOA.



Sign Up for Your New TripLOA Account !

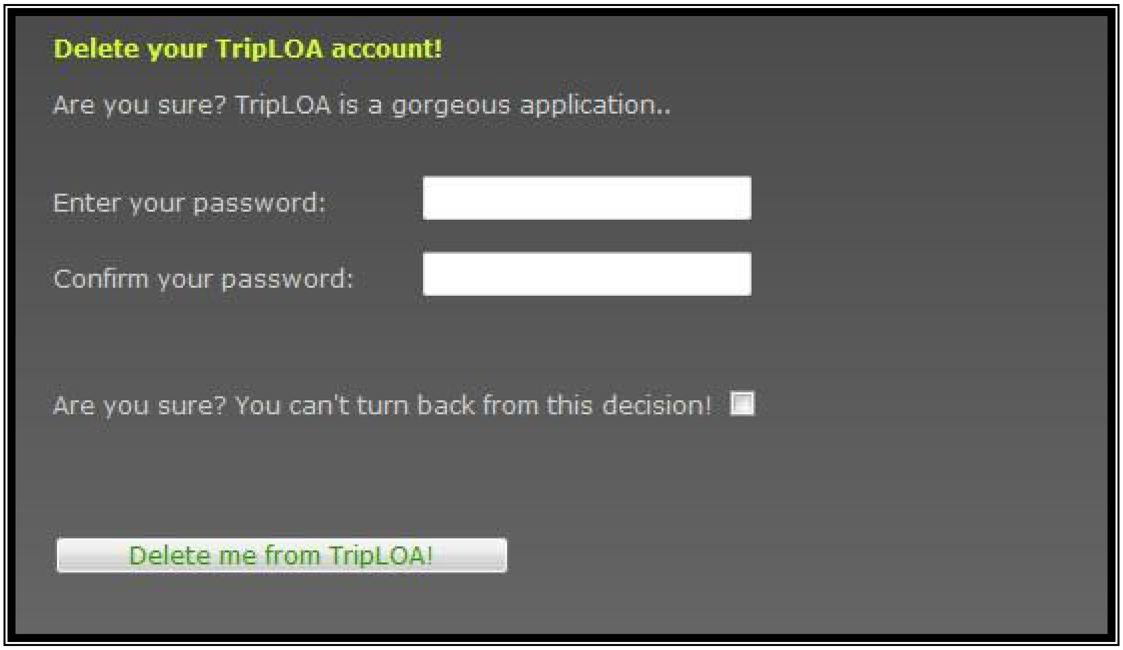
TripLOA User Name:	
Password:	
Confirm Password:	
E-mail:	
Security Question:	
Security Answer:	

The registration form is simple and light. An user can easily register to TripLOA, have a look to the application and fill his profile later. This is especially important if a user has to register through a mobile or a smartphone.

Delete an account

A user can delete his account from TripLOA. His username is not active anymore. His personal data are deleted, but some other information is still kept in the database in order to provider better general statistics. However, the informations that are left don't have reference to the identity of the deleted user.

The page for deletion is in /secure/deleteAccount.aspx. It is accessible through the "modify profile" pages. It looks like that:



Delete your TripLOA account!

Are you sure? TripLOA is a gorgeous application..

Enter your password:

Confirm your password:

Are you sure? You can't turn back from this decision! ☐

Password Management

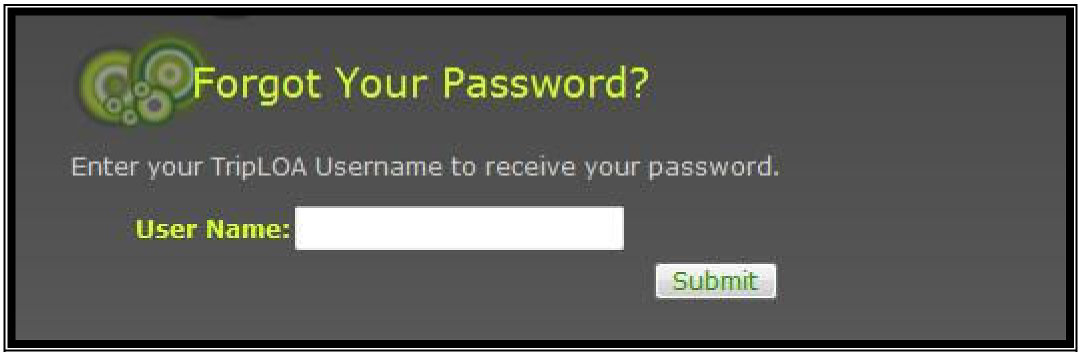
Password Recovery

It is not uncommon for people to forget their password. To account for this, websites that offer user accounts need to include a way for a user to recover his password. This process involves generating a new, random password and emailing it to the user's email.

This is the case of TripLOA. Passwords are stored in the database in a 'hashed' way.
So, if a user loses his password, the only way is to assign a new one to him. After receiving his new password, the user can log in and change his password from the randomly generated one to a more memorable one.

ASP.NET includes two Web controls for assisting with recovering and changing passwords. These controls work with the Membership framework behind the scenes to reset or modify users' passwords.

The PasswordRecovery control enables a visitor to recover his lost password.
The page containing this control is /passwordRecovery.aspx and it is accessible through the main menu :



Forgot Your Password?

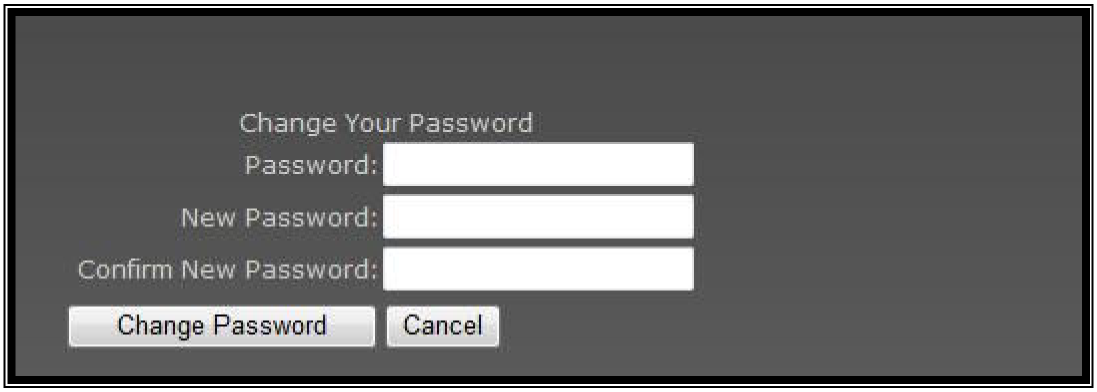
Enter your TripLOA Username to receive your password.

User Name:

It is simple: the user only has to insert his nickname. If he was registered to TripLOA, a mail will be sent to his address.
The template for the message is in the /common/mailtemplate.txt file.

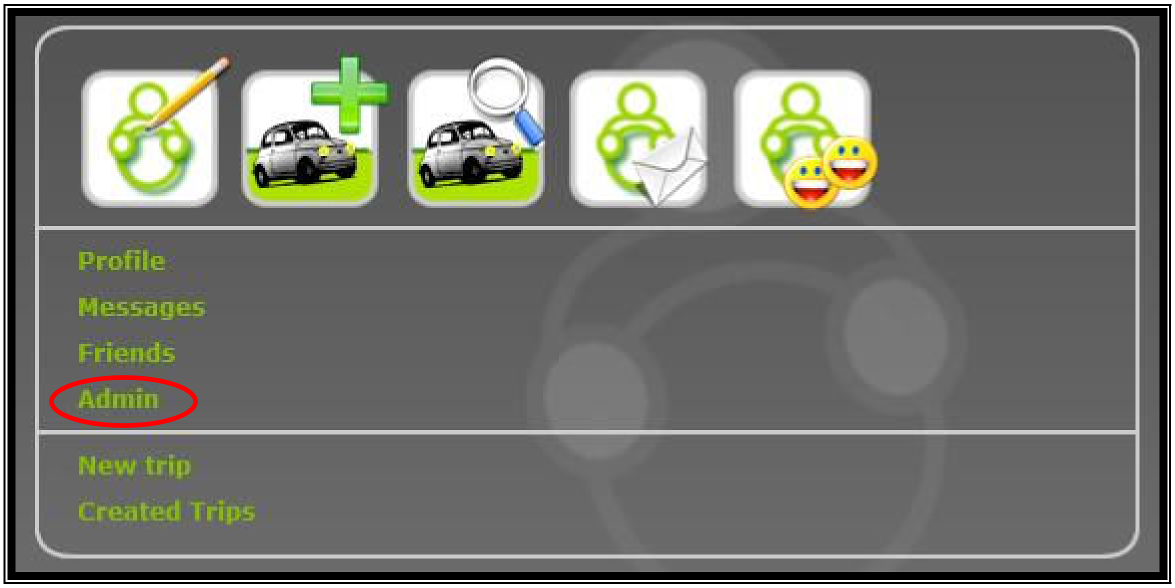
Changing Password

If a user wants to change his password, the ChangePassword control allows the user to update his password. This control is put in the /secure/changePassword.aspx page.



The new password is available immediately.

The administrator's pages

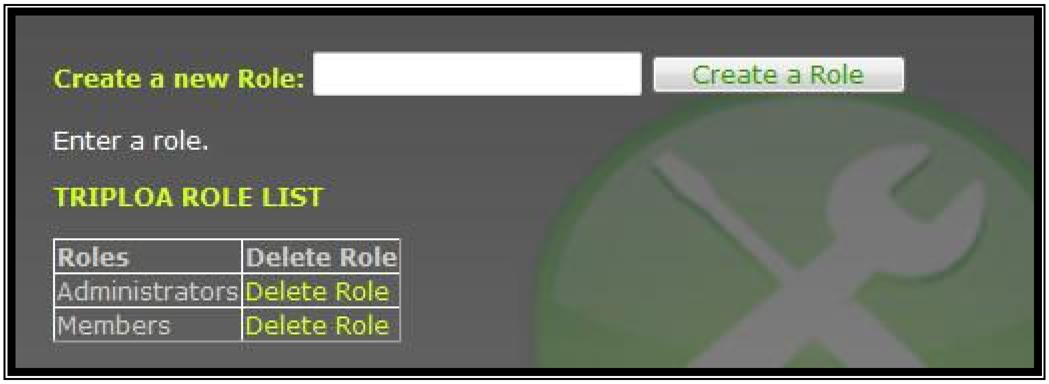


If an administrator logs in, his menu panel is augmented by a link to administration pages. His account shows the same features of 'members' users in order to do some tests and the 'admin' link, shown in the figure above, in order to reach Administrator features.

These features are divided into two main areas:

1. Roles Management (/roles/ManageRoles.aspx) ;
2. Users Management (/roles/ManageRolesToUsers.aspx).

Roles Management



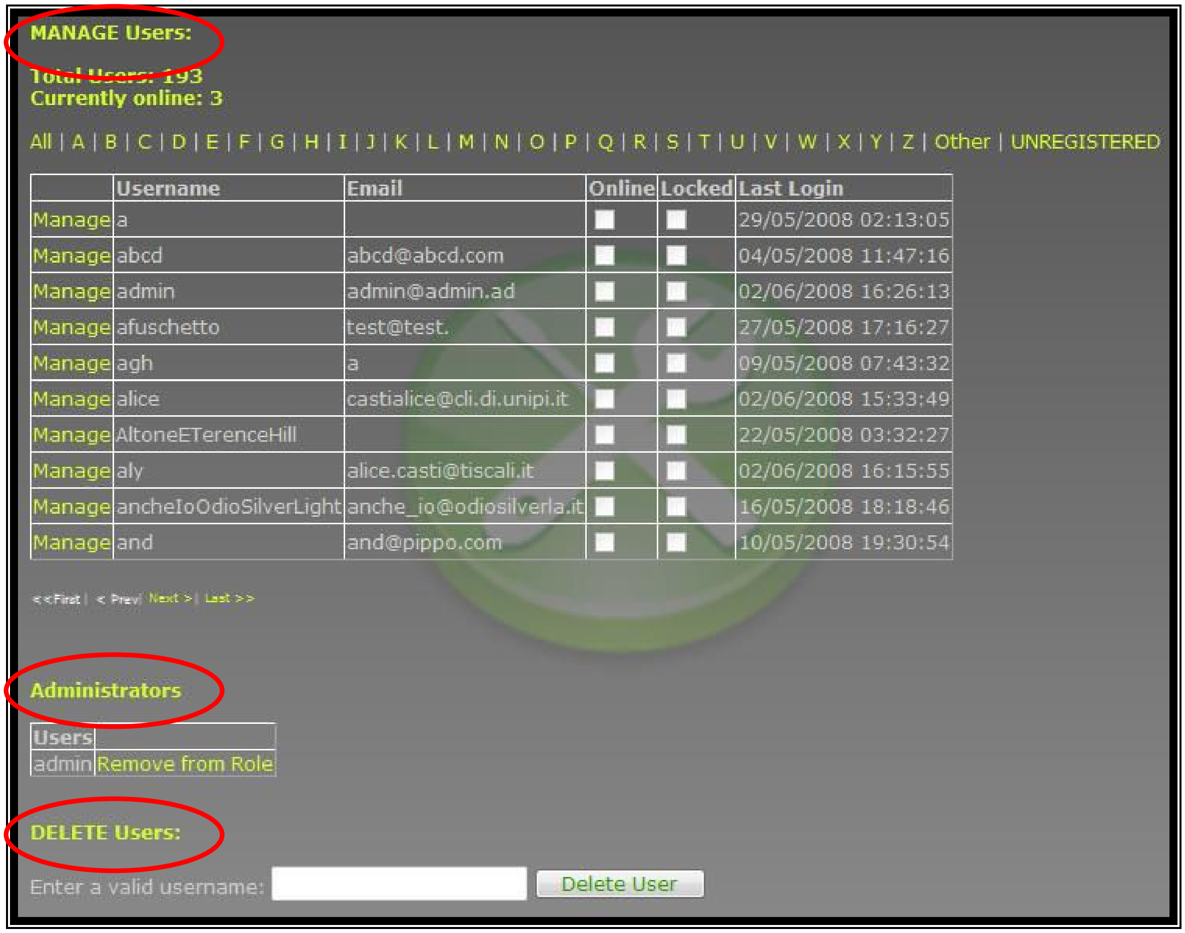
Enter a role.

TRIPLOA ROLE LIST

Roles	Delete Role
Administrators	Delete Role
Members	Delete Role

In this section the administrator can add or remove roles on order to create the basis for a new security policy in the application.
At the moment, TripLOA is configured to have two roles: Members, the role for normal users that register to the application and Administrators.
When a new account is created, its default role is “Members”.

Users Management



MANAGE Users:

Total Users: 193
Currently online: 3

All | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | Other | UNREGISTERED

	Username	Email	Online	Locked	Last Login
Manage	a		☐	☐	29/05/2008 02:13:05
Manage	abcd	abcd@abcd.com	☐	☐	04/05/2008 11:47:16
Manage	admin	admin@admin.ad	☐	☐	02/06/2008 16:26:13
Manage	afuschetto	test@test.	☐	☐	27/05/2008 17:16:27
Manage	agh	a	☐	☐	09/05/2008 07:43:32
Manage	alice	castialice@cli.di.unipi.it	☐	☐	02/06/2008 15:33:49
Manage	AltoneETerenceHill		☐	☐	22/05/2008 03:32:27
Manage	aly	alice.casti@tiscali.it	☐	☐	02/06/2008 16:15:55
Manage	ancheIoOdioSilverLight	anche_io@odiosilverla.it	☐	☐	16/05/2008 18:18:46
Manage	and	and@pippo.com	☐	☐	10/05/2008 19:30:54

<< First | < Prev | Next > | Last >>

Administrators

Users	
admin	Remove from Role

DELETE Users:

Enter a valid username:

This section is divided into three main areas:

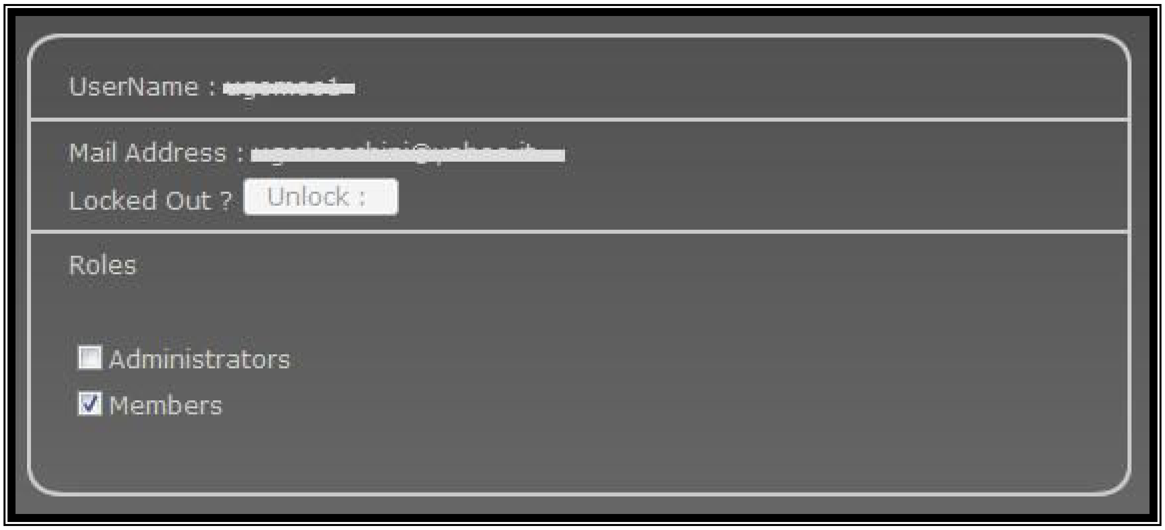
1. Manage users ;
2. Show administrators ;
3. Delete Users .

Manage Users

Users are displayed in a grid sortable by username. There are some data related to the user such as the mail address, on line status, last login date and also a locked out column.
In fact, all the architecture is configured to support a locking mechanism to prevent a malicious user from using brute force techniques to break into a user account. Too many bad passwords will lock out a user account and prevent the account from logging in, until the account is unlocked from an administrator. This policy can be tuned easily by settings the desired value of maxInvalidPasswordAttempts and passwordAttemptWindow in the web.config files in /Webconfigs folder .

The grid also shows those users that are not anymore registered to TripLOA.

The right column of this grid contains a 'manage' link. By clicking on it, an administrator can access a per-user personalized page (/roles/UserInformation.aspx).
The page is like this:



UserName : [redacted]

Mail Address : [redacted]

Locked Out ? Unlock :

Roles

☐ Administrators

☑ Members

Through this page, an administrator can unlock the user (if the user is locked, the unlock button becomes active) and assigning or removing roles to the selected user.
There are some checks that guarantee that the logged administrator cannot accidentally remove himself from the role 'Administrators'.

Show Administrators

A grid shows the administrators of TripLOA at the moment.
There are some checks that guarantee that the logged administrator cannot accidentally remove himself from the role ‘Administrators’.

Delete Users

A simple textbox permits an administrator to enter a username in order to easily delete the user. There are some checks that guarantee that the logged administrator cannot accidentally delete himself.