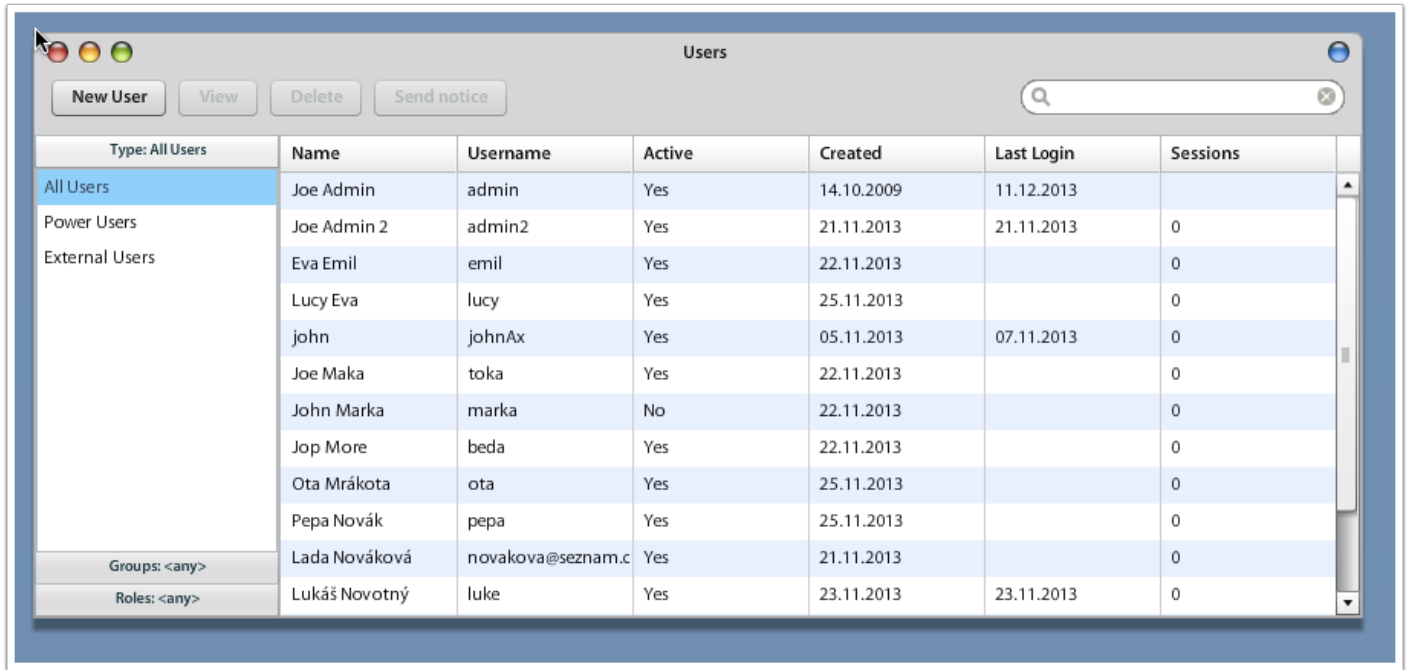


# Access Rights

- [Users](#)
- [General](#)
- [Implementation of Access Rights Best Practices](#)
- [Removing Users Accounts](#)
- [Events Access Rights](#)
- [Invoice Access Rights](#)
- [Options & Tools Access](#)
- [Groups & Roles](#)
- [User Profiles](#)
- [User Templates](#)

# Users

This page provides you with overview about Atollon Users database. You can filter for Power Users or External Users, as well as look-up users by their (Access) Groups or Roles.

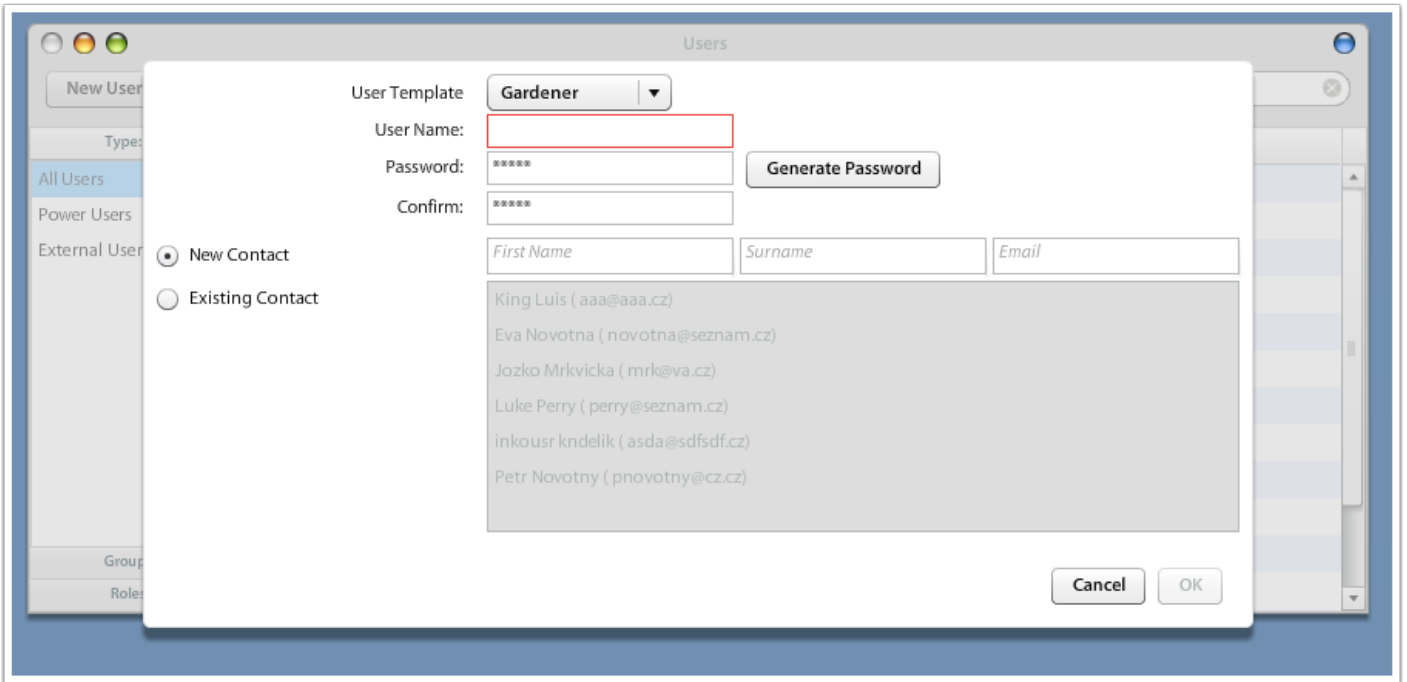


The screenshot shows a web application window titled "Users". At the top, there are buttons for "New User", "View", "Delete", and "Send notice", along with a search bar. Below the buttons is a table with the following columns: "Type: All Users", "Name", "Username", "Active", "Created", "Last Login", and "Sessions". The table lists several users, including "Joe Admin", "Joe Admin 2", "Eva Emil", "Lucy Eva", "john", "Joe Maka", "John Marka", "Jop More", "Ota Mrákota", "Pepa Novák", "Lada Nováková", and "Lukáš Novotný".

| Type: All Users | Name          | Username          | Active | Created    | Last Login | Sessions |
|-----------------|---------------|-------------------|--------|------------|------------|----------|
| All Users       | Joe Admin     | admin             | Yes    | 14.10.2009 | 11.12.2013 |          |
| Power Users     | Joe Admin 2   | admin2            | Yes    | 21.11.2013 | 21.11.2013 | 0        |
| External Users  | Eva Emil      | emil              | Yes    | 22.11.2013 |            | 0        |
|                 | Lucy Eva      | lucy              | Yes    | 25.11.2013 |            | 0        |
|                 | john          | johnAx            | Yes    | 05.11.2013 | 07.11.2013 | 0        |
|                 | Joe Maka      | toka              | Yes    | 22.11.2013 |            | 0        |
|                 | John Marka    | marka             | No     | 22.11.2013 |            | 0        |
|                 | Jop More      | beda              | Yes    | 22.11.2013 |            | 0        |
|                 | Ota Mrákota   | ota               | Yes    | 25.11.2013 |            | 0        |
|                 | Pepa Novák    | pepa              | Yes    | 25.11.2013 |            | 0        |
|                 | Lada Nováková | novakova@seznam.c | Yes    | 21.11.2013 |            | 0        |
|                 | Lukáš Novotný | luke              | Yes    | 23.11.2013 | 23.11.2013 | 0        |

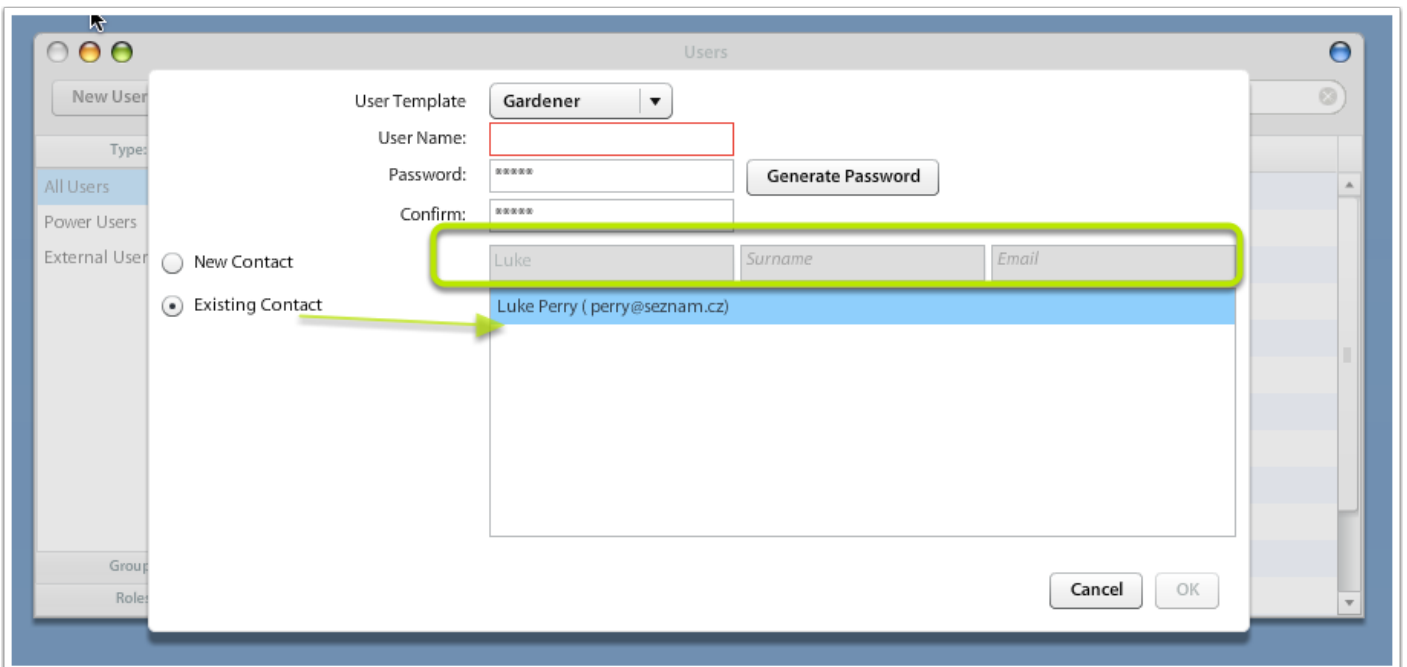
## Create New User

You can create new user based on any (existing) User Template. In case there are no templates available, you can create new using Options & Tools > User Templates.



## Create new contact vs. select existing

You have option to create new contact for newly created user or if you know there is already user's contact in your database, you can search for the existing contact. Just write person's First Name, Surname or E-mail & switch to "Existing Contact" option. Application should filter for your contact. In case the contact is not user yet, you'll be able to select existing contact, to which the new User account will be associated.



## User Base Types

Power User

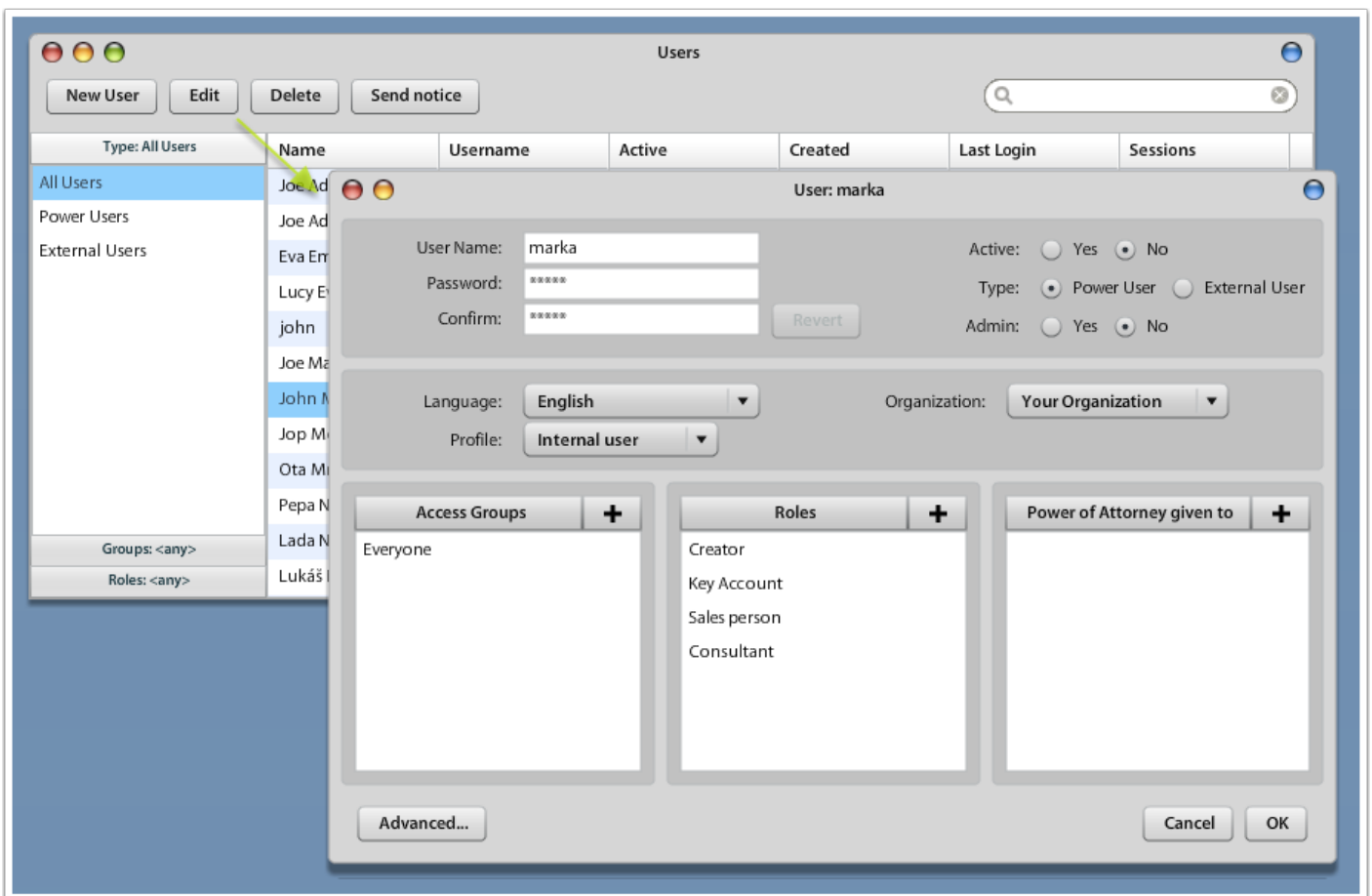
Power User is internal, fully licensed user, whom you may add any rights to use Atollon in it's full potential.

## External User

External User is free, restricted user. The conditions for using this type of users are restricted by Atollon Company.

See how to [add new User](#).

## User Edit Details



## User Fields

### User Name

Indicates the user in the system. You can rename this field at any time and it will not have effect on Atollon (all records, where the User Name was indicated will be renamed at the same time).

**If you want to change users first name and surname (contact name) you can do it in contacts. Open contacts, find specified contact that belongs to the user and change the name there.**

## Password + Confirm

Fill-in the User's Password and confirm it (write the same password once more).

## Active (Yes/No)

Indicates whether the user can login to system and whether it will be available to other users.

## Type (Power User/External User)

Switch whether the User is regular (Power) user or whether it is your limited (External) user, for example client or partner.

## Admin (Yes/No)

Indicate whether this user will have access to administration features. Some Atollon features may be accessible only to administrators.

## Language

Indicate preferred user's language for the application interface. Some Atollon features provide (by default) multi-lingual information in user's language. Please note that in communication with users using Mass Mail or Workflow, Preferred Language on contact is used instead.

## Organization

Default Organization (for Atollon set-up in multi-organization mode).

## Profile

User's default application interface behavior.

# User's Access Rights Options

## Access Groups

Add the user to one or more Access Groups to assign the user immediately permission to selected modules, functions and data. By default, there are several access groups pre-configured to meet general needs. More advanced users may customize Atollon access rights fully using Atollon Windows Administration interface.

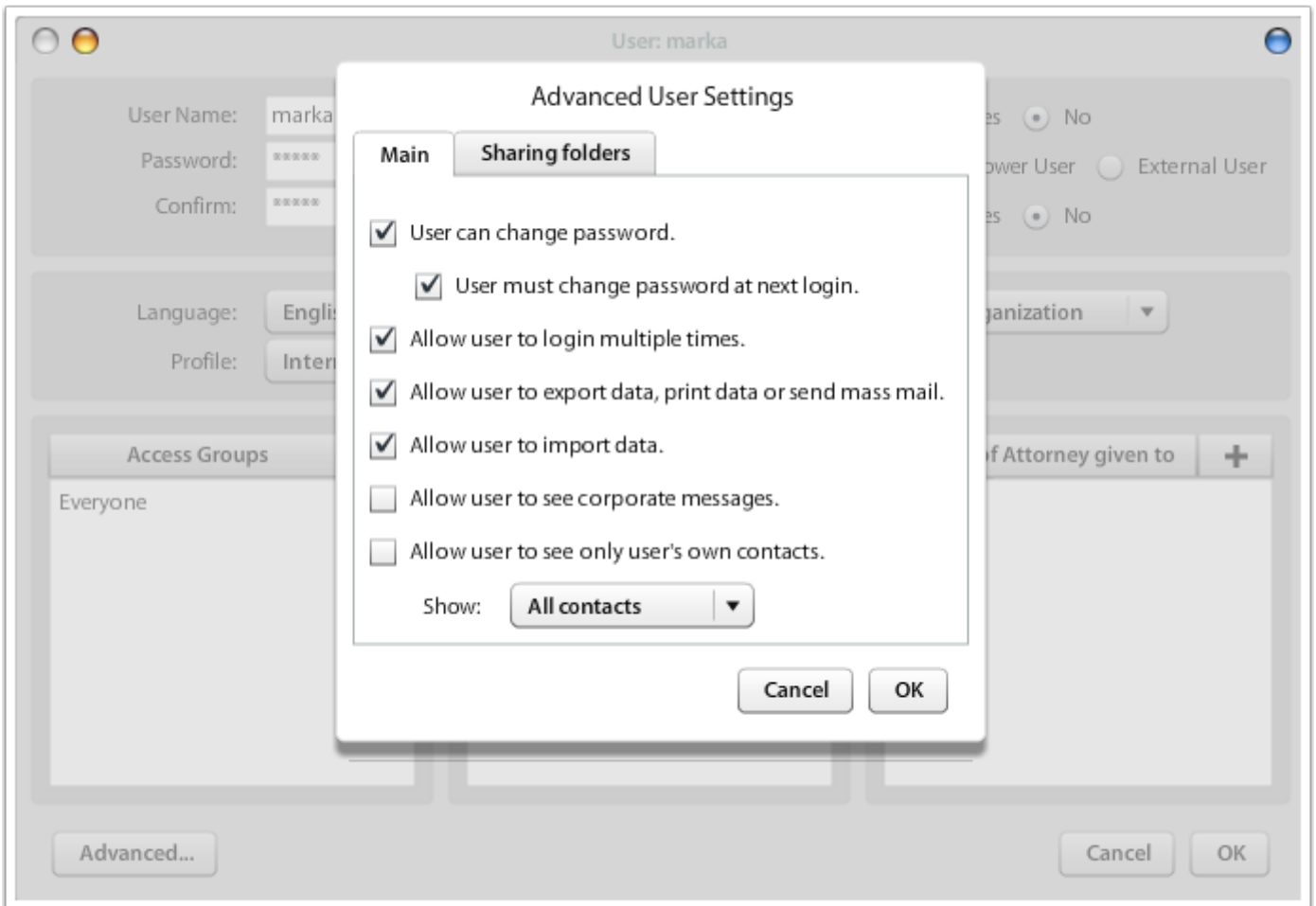
## Roles

Allow the user to occupy one or more Roles. The user is authorized to use Role's permission only once the user is added to the same Role on Project or Atollon's Folder.

## Power of Attorney given to

This option allows you to add this user's rights temporarily or permanently to some other user(s). It may be useful once the user gets on vacation, to give some other people her access rights for the same time. Please note that also personal data are available in the same time, incl. calendar, tasks & messages.

## Advanced Options



### User can change password

Otherwise user can't

### User must change password at next login

The user will be required to change their password after logging in. This is a necessary step for [setting up a calendar on an iPhone](#).

### Allow user to login multiple times

Should the user be able to login several times to Atollon? If not selected, the user will destroy all open sessions, when logout.

## Allow user to export data

Should the user have possibility to use export functions?

## Allow user to import data

Should the user have possibility to use import functions?

## Allow the user to see only user's own contacts

What are user's own contacts?

- User created the contact
- User edited the contact
- User is primary responsible for the Account (Contact Folder)

## Sharing Folders

This options allows user(s) to share folders with another organization.

Example:

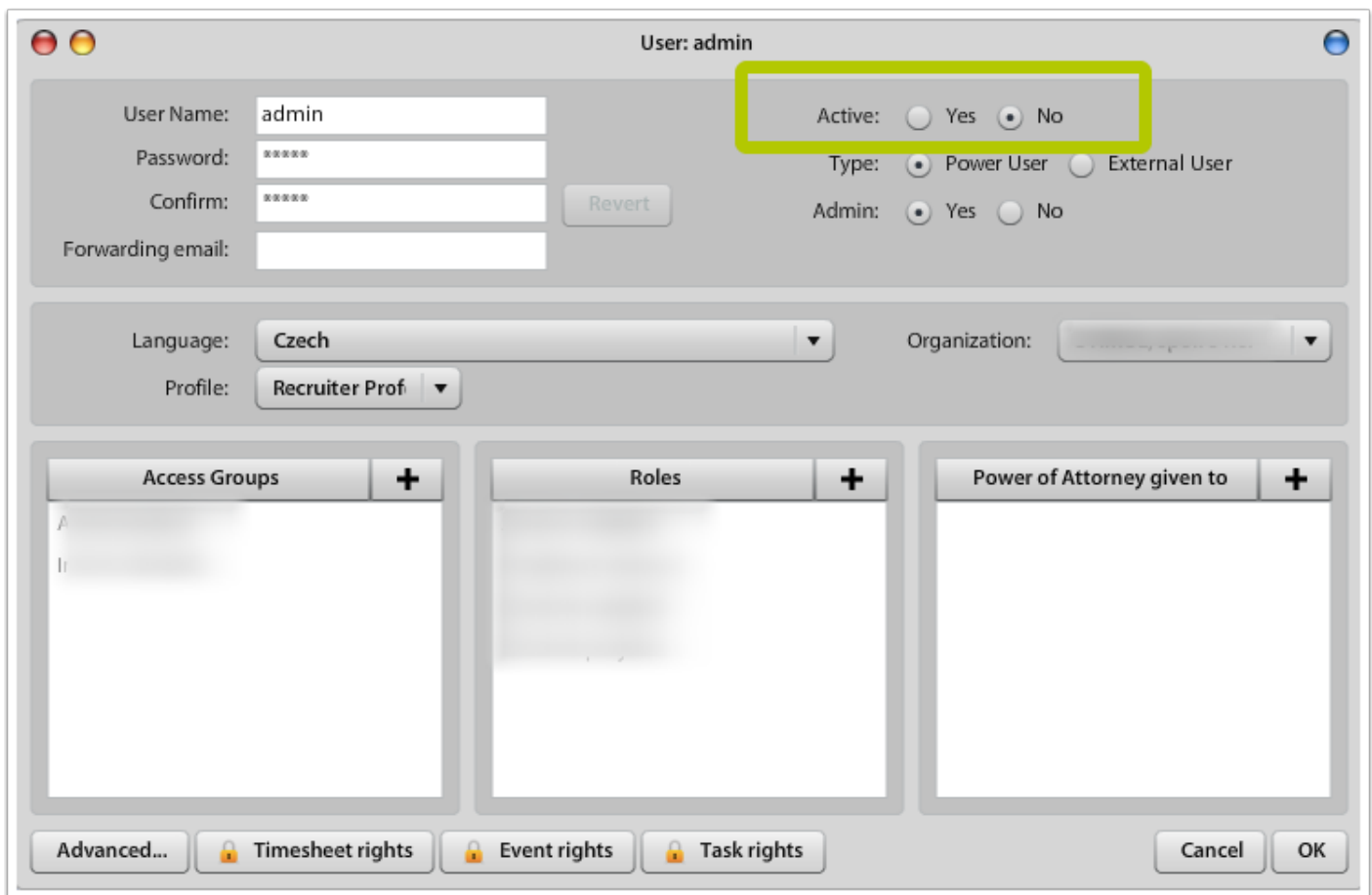
- Organization A (Legal services): Clients (separate)
- Organization B (IT Support): Clients (separate)
- Both Organization A + B: Prospects (shared database of potential customers coming from web)

*(Note to Atollon consultants: When setting-up organizations, please make sure that in order for system to work properly, it is necessary to share Folder (Type, Template, Status, Forms, etc.) settings.)*

# Remove or Deactivate User

## Temporary block user account

1. Options & Tools -> Users -> double click user -> set **Active** option to No.
2. [Redirect existing mail address](#)



## Permanently remove user account

1. Options & Tools -> Users
2. Select the user & Delete

Please be aware that by deleting the user you won't be able to filter for user's records any more (incl. any Time Sheet records she created, Projects, Clients, etc.) In case the user has track record that should remain in the system, do not delete the user, instead just make the user inactive (so it can be activated temporarily, if necessary).

User is never technically deleted from the database. In case you accidentally deleted the user record and need to return it to it's previous state, you may contact Atollon technical support for help. Please note that this operation requires server restart and is enabled only on dedicated Atollon instances.

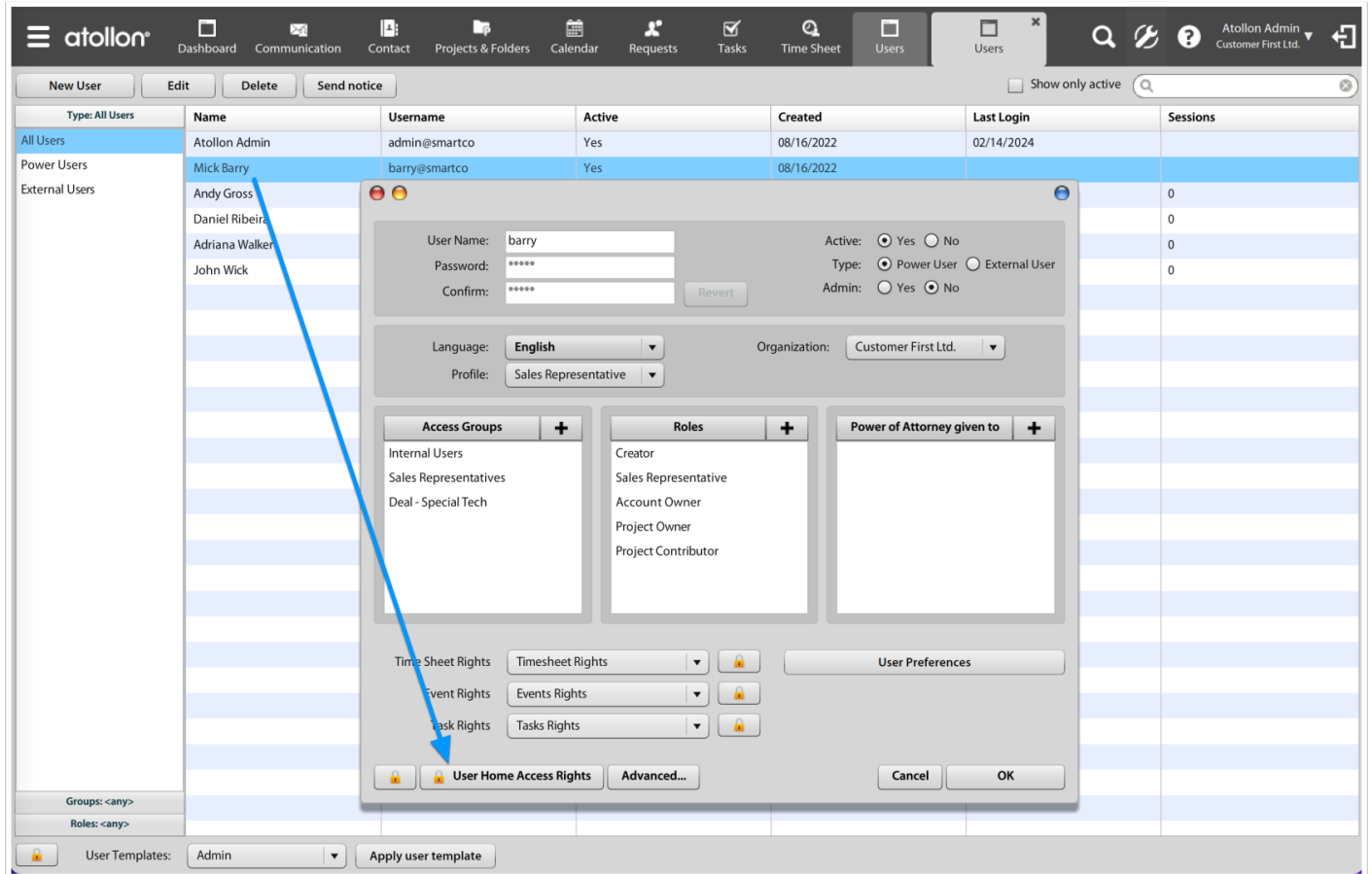
## User Home Privacy

Each user get her own **User Home** folders that may contain private (personal) messages, private e-mails, private documents, etc.

By default Atollon shares all communication within company. If you want to avoid sharing personal data, you should verify User Home settings and disallow inheriting global rights.

# Check User Home rights

Go to Options & Tools > User. Open detail of each of the users. Open User Home Rights.



# User's Home Folder Rights

After clicking **User Home Rights** button, you get to see rights of user's mail inbox. Look at what rights are inherited from parent ACL tree nodes, until you get to **user@instance** folder ACL settings (**user@instance** will contain your user's username, such as **barry@smartco** on below screenshot).

The screenshot shows a user management interface with a modal window for editing ACLs. The modal window is titled "Edit ACL TREE00000003803 User Home > barry@smartco > Messages > My Messages". It contains a table with the following data:

| Label   | C... | Change ri... | Mandator... | ACL Links  | R... | E... |
|---------|------|--------------|-------------|--|------|------|
| default | or   | LVNEDRAuAd   |             | TREE00000003801 User Home > barry@smartco > Messages | X    | 🔒    |

A blue arrow points to the red 'X' icon in the 'R...' column. A black callout box with white text says "Go to parent level until user@instance folder (2x up)". Below the table are tabs for "Simple" and "Advanced", and a section for "Users" with a table listing "Atollon Admin" with "View", "Edit", "Delete", and "Full" rights checked. The modal also shows "Current rights: LVNEDRAu" and "Cancel" and "Save" buttons.

## Remove user's folder global rights

Once you get to **user@instance** ACL settings (see highlighted title on screenshot), you may remove the inheritance of this user's folder to it's parent (User Home folder).

Before saving, you need to add the **User's own Full rights** (they should be already preset) and **Administrators** full rights (they may be missing). If you want to avoid Administrator's rights to user's home folder, you need to make this configuration under **root** user. That is the only user, who may limit access rights to anyone except the User Home folder owner.

atollon® Dashboard Communication Contact Projects & Folders Calendar Requests Tasks Time Sheet Users Users Atollon Admin Customer First Ltd.

New User Edit Delete Send notice Show only active

| Type: All Users | Name          | Username      | Active | Created    | Last Login | Sessions |
|-----------------|---------------|---------------|--------|------------|------------|----------|
| All Users       | Atollon Admin | admin@smartco | Yes    | 08/16/2022 | 02/14/2024 |          |
| Power Users     | Mick Barry    | barry@smartco | Yes    | 08/16/2022 |            |          |
| External Users  | Andy Gross    |               |        |            |            | 0        |
|                 | Daniel R      |               |        |            |            | 0        |
|                 | Adriana       |               |        |            |            | 0        |
|                 | John Wi       |               |        |            |            | 0        |

Edit ACL TREE00000003797 User Home > barry@smartco

| Label   | C... | Change ri... | Mandator... | ACL Links                  | R... | E... |
|---------|------|--------------|-------------|----------------------------|------|------|
| default | or   | LVNEDRAuAd   |             | TREE000000002763 User Home | X    | 🔒    |

Remove access rights inheritance from user's home folder

Simple Advanced

Users: + Add User - Remove User

|        | Name       | View | Edit | Delete | Full |
|--------|------------|------|------|--------|------|
| Groups | Mick Barry | ✓    | ✓    | ✓      | ✓    |

Verify Administrators group access rights to user's home folder

Current rights: LVNEDRAu

Cancel Save

Groups: <any>  
Roles: <any>

User Templates: Admin Apply user template

# General

## Atollon Directory

Access Rights in Atollon server are based on tree-hierarchical structure. See the attached document for the Atollon Directory scheme.

## Roles

**Role** is **Access Rights** entity that can be assigned to users in connection to **Folder (Account)** or **Project**. **User** must be allowed to fit into specific role. See **User Settings** to add user into role. By adding user into role, you specify that anyone with R (Rights) permissions can assign the **User** into the **Role**. Nothing else. **User** does not get any rights only by adding the user into the **Role** (this is different compared to **Access Group** rights). **User** gets permission specified by **Role** rights only after *Account Manager*, *Project Manager* or any other authorized **User** adds the user into **Role** on **Project** or **Folder** (Account).

## Role "Creator"

**Creator** role is specific system-generated **Role**, which helps assign User into **Creator** role automatically after creating the **Folder** (Account) or **Project** based on **Folder / Project Template**.

## Define Project Role Rights

**Project Template (Folder Template)** may define specific access rights that any **User** assigned to **Project Role** on specific **Project** may receive. To amend **Project Role** rights, go to **Project Template Settings** and change **Custom Rights** options. These rights are pre-definable only to new projects. If you want to change rights to existing projects, you should check function of mass-project rights change in **Reporting** (only Win client).

If the **Project Role** rights are not specified by **Project Template**, but are allowed by **Project Type**, system automatically assigns full rights to the user on the project.

# Conditions of adding User to Role on Project

1. Check whether **User** may be assigned to **Role** (see User Settings)
2. Check whether **Project Type** contains the specific **Role**
3. Check whether user assigning other users has **R** (Rights) permissions on the particular **Project**.

Please be aware that usually projects are visible (editable / approvable) also by **Access Group** rights to large number of users (*Project Managers, Administrators, Everyone*, etc.) depending on **Project** default access rights settings (based on **Project Template**).

## Access Rights Properties

### ACL (Access Control List)

Atollon system access rights utilize per-object access rights. That means each Container or Leaf Node may have it's own Access Rights definition.

### Access Rights Definition

Users, Groups and Roles may be assigned to have authorization to **List, View, Create, Edit, Authorize** or amend **Rights** of each individual object that is associated to the ACL. Special rights include **Admin** (this right can be editable by root user only and disallows changing this permission to any other users) and **Finalize** (this right means that the permission is set for the current object only and can not be inherited).

### Access Rights Inheritance

Access Rights to one object (ACL) may be automatically taken from another ACL (or multiple ACLs). This is used when setting-up rights for more records (messages, documents, etc.) at the same time. It is enough to set rights in parent node / folder / container and the objects linking to this container will get the same rights as the container itself.

**Example:** Set that the group Everyone will see the project "Company Party". Any message or document created/uploaded under project "Company Party" gets the same rights as the "Company Party" project, because the new message/document has ACL that links to it's parent (the project folder).

## How is the inheritance ensured?

Rights are automatically inherited, because they are (usually) created based on Template ACL. The Template ACL is the object's property that holds the definition of new (child object) ACL to be created. This Template ACL, by default has set that the newly created (child) objects will link to it's parent (current object).

## Multi-link ACL

Some records, such as Folders, Projects, Activities or Invoices are multi-linked. That means their ACL is inherited from several parent nodes, incl. for example **Folder Type and Parent Folder** (in case of Folder). When linking rights, **filters** are applied. That means that in order to get L, V rights to the Folder, you have to have L rights to it's parent, etc.

## Are there any exceptions?

Yes, in Project or Folder Templates, administrators may set-up different behavior for creating new ACLs for newly created Folders & Projects. They may change the Template ACL to link to different container and in that way change default rights of various Folders & Projects, based on selected Folder or Project Template.

## How to check what rights are inherited?

You just open the ACL detail and click on "Show linked rights". The condition is that the ACL links to other ACL.

## How do I avoid inheritance

You can either change this in Template ACL (remove the linking) or you can change it on already created object (again, remove the linking). You can not remove rights that were set as Admin. Those can be removed only by super user.

## Proxy Rights

Proxy Rights are used to temporarily or permanently give rights of one user to another. To set-up Proxy Rights, you must open User's details (the one that give the Power of Attorney) and add the other user (the one who will get those rights).

Example: Person leaves for vacation and you want other user to take over the responsibility in the time of absence. Go to the absent user's details and add full Power of Attorney to another user. Please note that this change is global, therefore it affects also the user's personal messages and documents.

Enable:

Edit events in other users calendar: Need access on other users timesheets

Conflict: If enabled editing callendars also editing timesheets is enabled and vice versa

Disable:

## Found proxy connection

there is script what found you all proxy use on virtual server instances:

[listProxtThroughDatabases.sh](#)

move him to /tmp/, su postgres and run:

```
sh /tmp/listProxtThroughDatabases.sh
```

Output looks like:

```
database |      id      | username | proxyid | proxyname
-----+-----+-----+-----+-----
harfonie | 190086000 | snadova  | 67385000 | rytova
harfonie | 190099000 | marsala  | 67385000 | rytova
harfonie | 1099228000 | hamalova | 190099000 | marsala
```

# Implementation of Access Rights Best Practices

Template implementations have some of the access rights preconfigured. Any other access rights may be customised for individual client's needs.

## User vs. Group Access Rights

When defining new access rights, please rather use **Groups** instead of **Users**. Users and their roles may change time from time, so it would be easier to hand over the role in the company to someone else just by changing user's group membership.

## Assign User to Groups

### Power Users

All Power Users should be placed into group **Everyone** or **Internal** at least.

All Power Users should be placed into role **Creator** & role based on person's working relationship to the company.

All Power Users should be set to one Profile (used for GUI) - the default is based on template.

### External Associates

All External Associates should be placed into group **External Users**.

All External Associates should be set to one **Profile** (used for GUI) - the default is based on template.

### Clients

All Clients should be placed into group External Users.

All Clients should be set to one Profile (used for GUI) - the default is based on template.

# Access Rights to Estimates, Invoices, Orders

All access rights are based on the group access rights level set-up for each individual node in Atollon Directory Administration.

## Estimates, Invoices, Orders

Estimate / Invoice Approver

Estimate / Invoice / Order Editor

Estimate / Invoice / Order Reader

## Time Sheet

Timesheet Approval group - users enabled to see / approve timesheets of other users.

# Removing Users Accounts

## Temporary block user account

1. **Options & Tools** -> Users -> double click user -> select "No" from active Radio Buttons
2. Redirect existing mail address

## Permanently remove user account

Please note that user accounts are never permanently deleted, there must always track dent of the user existance in the system. We recommend to deactivate user's account rather than deleting it. It may be difficult to restore once deleted user account. Also, sometimes you might want to use user for reporting. In case you delete the user completely, it might be difficult to report on user's records (Time Sheet data, Invoices, Folders & Projects, etc.).

1. Options & Tools -> user accounts -> double click user ->
  - a) set Active combo box to No,
  - b) change its passwords,
  - c). remove user from all groups and roles,
  - d) **don't delete that user account.**
2. Redirect existing mail address
3. Remove its mailbox.
4. Find user in contacts (you might see users contact name in users table under Setting -> Access -> Users -> Contact column)
  - a) right click that contact -> Edit -> go to tab Others,
  - b) remove relationship to System user by clicking the "C" button.

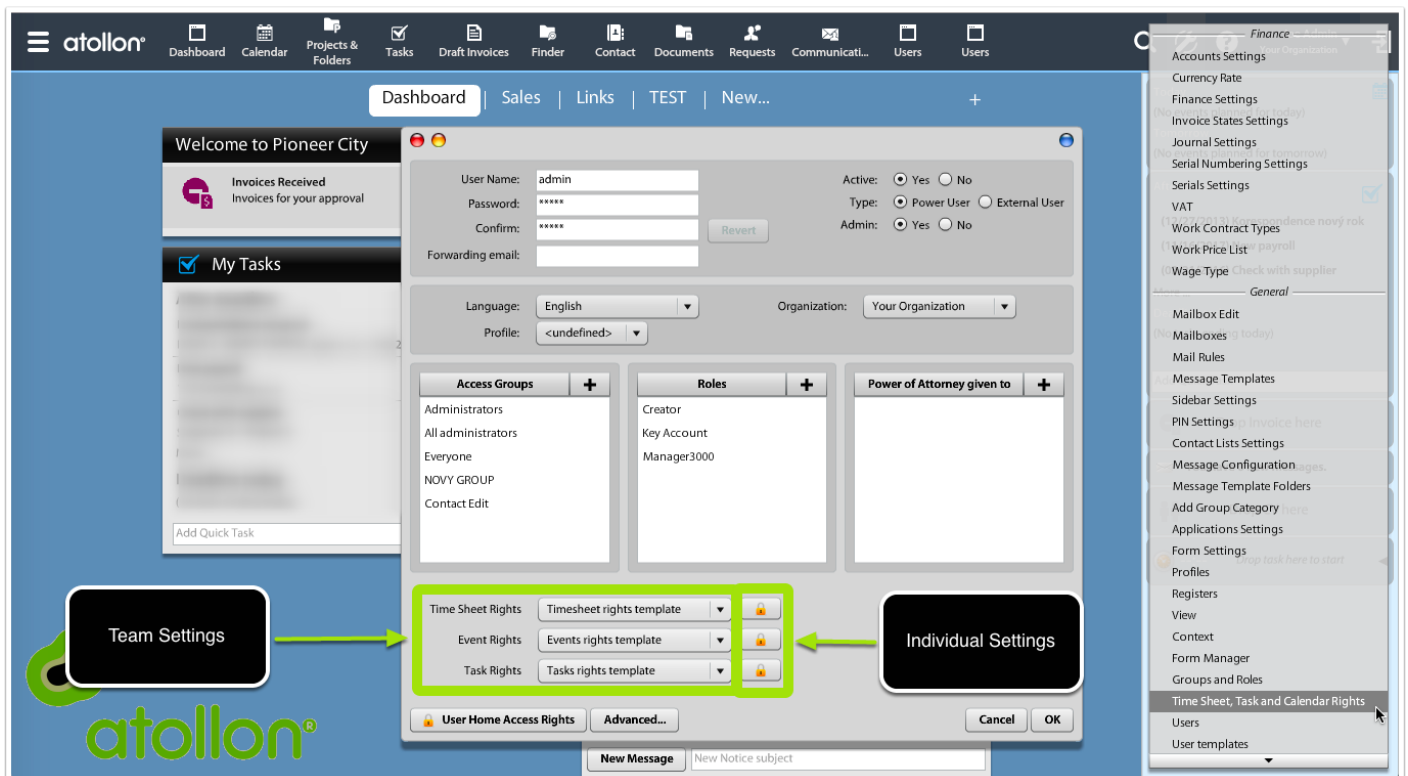
# Events Access Rights

## General

**Tasks, Events** and **Time Sheet** records have rights calculated by combination of rights to context (Folder, Project or Activity on which the Task is stored) and rights of User's Event, Task, TS rights. s

## Rights to User's Events, Tasks, Time Sheet

**Each user may authorize other users** to create / edit / read / delete / authorize their Calendar Events, Tasks or Time Sheet records. This setting is usually setup by system administrator.



Go to **Users > User detail** screen. In the bottom part, you have 2 options how to edit right of any users to selected user's Events, Tasks or Time Sheet entries:

## Individual Settings

You can set who may create or modify records belonging to particular users.

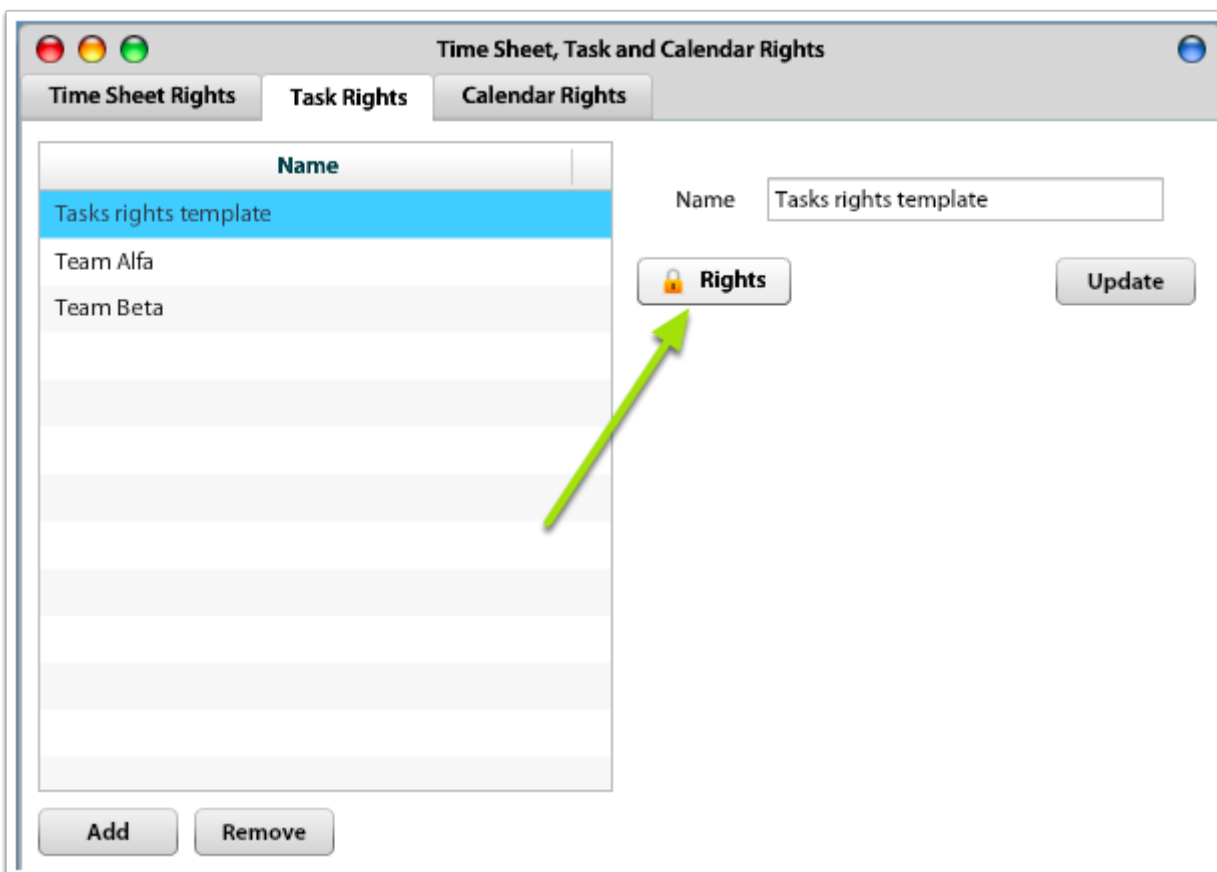
## Team Settings

You may create Rights Templates for Events, Tasks and Time Sheet Entries. These templates are usually created to hold team members that have access to colleague's records.

# Advanced Team Access Rights Configuration

## Event, Task, Time Sheet Rights Templates

In order to keep rights to records in good order for company teams, it is possible to create any number of Rights Template for Tasks. Each team member's User settings would be selected with "Team Alfa" access right template for Tasks. In this setup, anyone having the access to the Tasks Rights Template called "Team Alfa" would get access to any user in the same team. We expect that access group "Team Alfa" would be created and the rights of this group would be added to the Task Rights template.



To set-up teams, follow the procedure:

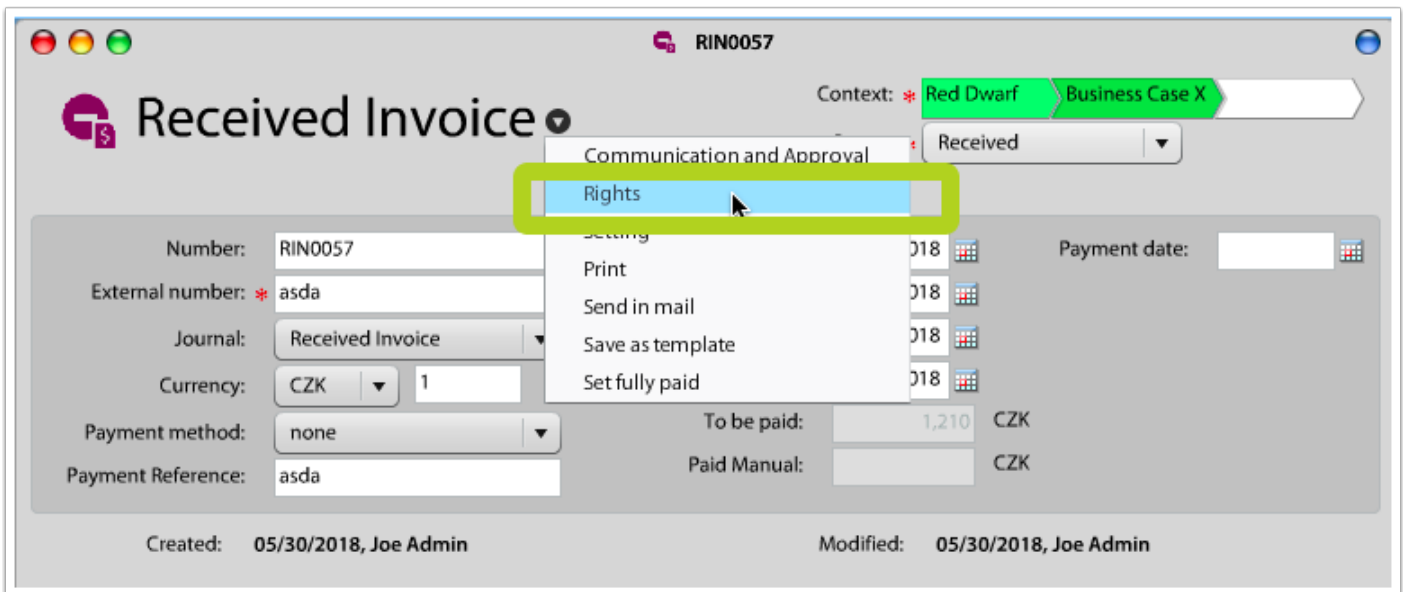
1. Create Access Group "Team Alfa"
2. Create Task Rights Template "Team Alfa Rights"

3. Add "Team Alfa" Access Group to "Team Alfa Rights" container (see the picture above)
4. Update User to have Task Rights template set to "Team Alfa Rights"

# Invoice Access Rights

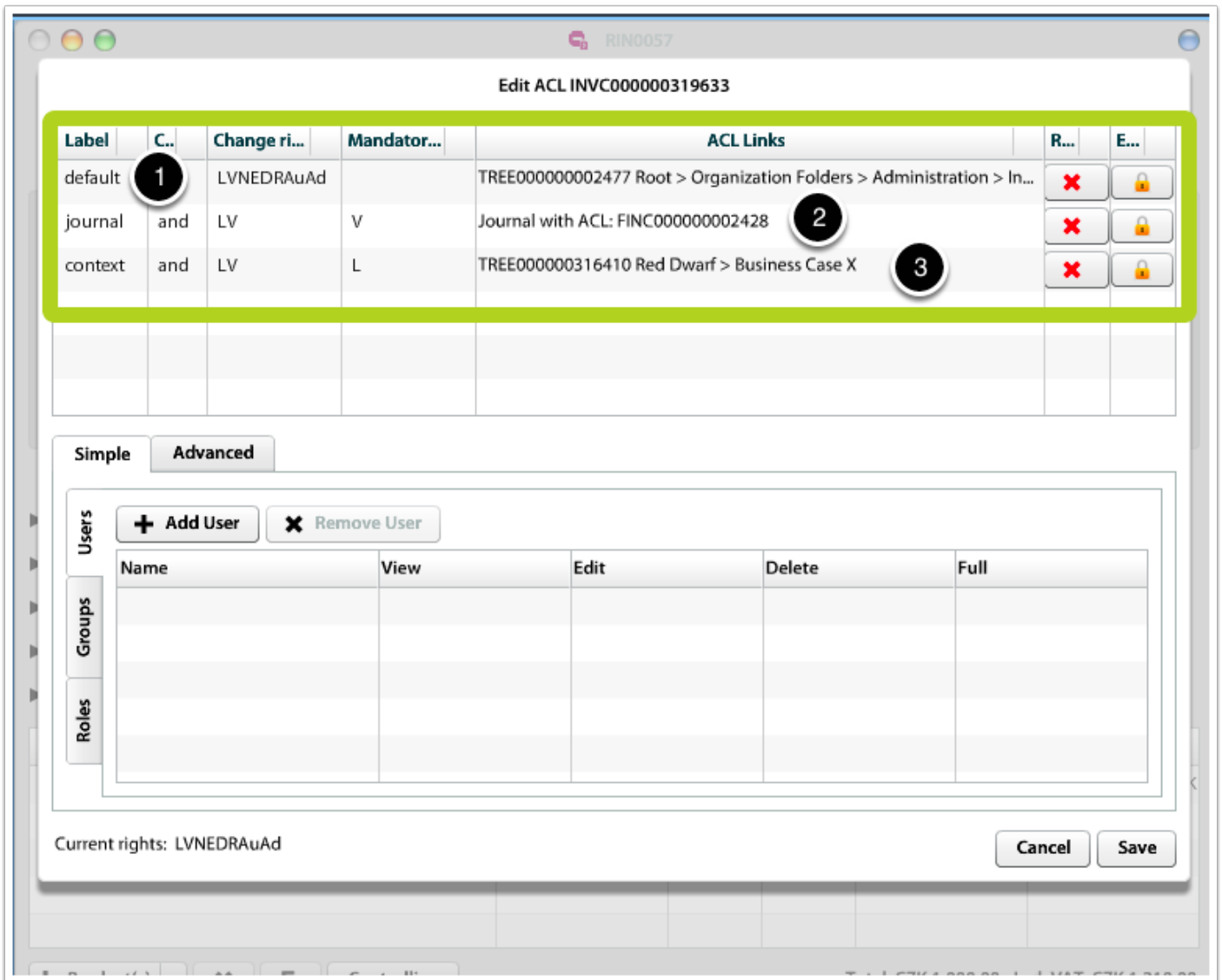
Each Invoice has its own ACL (information about who can access the record). That means, each individual Invoice may have different access rights. This behavior is used when sending Invoice for approval. Each approving user is automatically assigned appropriate **edit** rights to approve the invoice.

## Edit Individual Invoice Rights



## Default Invoice Rights

Invoice's rights are inherited from 3 different parent ACLs.



# 1) Invoice Administration Node

Each Invoice application (Invoice Issued, Invoice Received, Purchase Order, Received Order, Estimate) has its own administration node that takes care about default access rights to all Invoices stored to this particular node. As mentioned in the "Change Rights" filter (see screenshot), all rights of the Invoice node are inherited by the individual invoices.

In case you want to allow users read / write invoices, add their Access Group to the Invoice administration node. You can do this by clicking on "lock" button next to the first row (where Label = default).

# 2.) Journal

Each Invoice (or other document from invoice module) has Journal (such as "Domestic Invoices" or "Foreign Invoices" or "Secret Invoices"). In order to allow users see any invoice that is in "Secret Invoices", the user must have the VIEW rights to the Journal. In case the user does not have VIEW

rights on "Secret Invoices" journal, she won't see these invoices. This works even if the users sees all other invoices...

In order to edit Journal access rights, you may directly get to the configuration using "Lock" button next to 2nd row (where Label = journal) or you may go to Options & Tools > Journal Settings > Edit each journal and set the desired access rights.

## 3.) Context

Each Invoice (based on it's header) may be stored to any **context** (Folder, Project or Activity). The user must have LIST rights on the context (Project, where the invoice is stored) in order to get the READ (L, V) rights to the invoice. For example, if the user has rights to "Secret Invoices" based on the invoice journal, but does not have L rights to "Super secret project", the user won't see such invoice.

# Invoice Approval Rights

Invoice approval rights are administered using **Journal settings**. The user must have L, V, E rights in order to approve the invoice. The user **must NOT have Authorize** right in order to use the rights defined by Journal settings. Users **having** Authorize right (based on invoice ACL) are **super users**, who may approve or change invoice status to any status **ignoring** the Journal settings.

# Options & Tools Access

We display settings in Options & Tools menu based on user access rights to particular setting. The following list describes most of the setting options and what rights the user must have to see these settings. This information is necessary for administrators to set-up settings visibility properly for all users.

## Settings visibility

| Settings Option        | Who can see                 | What node is checked          |
|------------------------|-----------------------------|-------------------------------|
| VAT                    | verify access rights (Edit) | FINANCESETTINGSNODE           |
| Work Contract Type     | verify access rights (Edit) | WORKCONTRACTSNODE             |
| Wage Price List        | verify access rights (Edit) | PROJECTPRICINGNODE            |
| Wage Type              | verify access rights (Edit) | WAGEREPORTNODE                |
| Mailboxes              | verify access rights (Edit) | MAILBOXESNODE                 |
| Message Templates      | verify access rights (Edit) | MESSAGETEMPLATESNODE          |
| Add Group Category     | verify access rights (Edit) | DISTRIBUTIONGROUPCATEGORYNODE |
| Profiles               | show to Admin only          |                               |
| Registers              | show to Admin only          |                               |
| View                   | verify access rights (Edit) | VIEWSETTINGSNODE              |
| Activity Panel Presets | verify access rights (Edit) | ACTIVITYPANELNODE             |
| Activity Panel         | verify access rights (Edit) | ACTIVITYPANELNODE             |
| Context                | verify access rights (Edit) | SUBJECTTYPECODE               |
| Users                  | verify access rights (Edit) | USERNODE                      |
| Background             | show to Admin only          |                               |

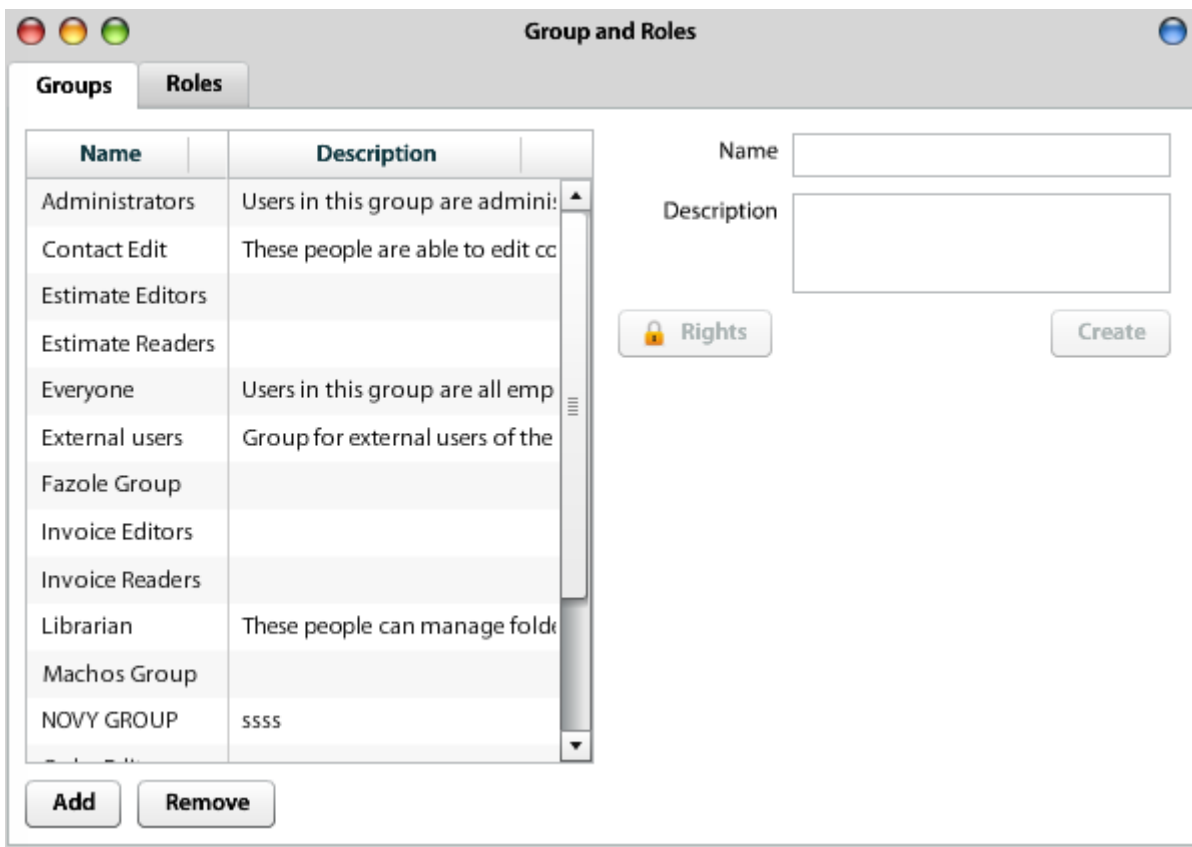
| <b>Settings Option</b>    | <b>Who can see</b>          | <b>What node is checked</b> |
|---------------------------|-----------------------------|-----------------------------|
| Dimension Settings        | verify access rights (Edit) | DIMENSIONSNODE              |
| Workflow Actions          | verify access rights (Edit) | WORKFLOWSETTINGSNODE        |
| Workflow Filters          | verify access rights (Edit) | WORKFLOWSETTINGSNODE        |
| Workflow                  | verify access rights (Edit) | WORKFLOWSETTINGSNODE        |
| International             | show to all                 |                             |
| Manage Print Templates    | show to Admin only          |                             |
| About Lagoon              | show to all                 |                             |
| Logger                    | show to all                 |                             |
| Event Workflow            | verify access rights (Edit) | TASKWORKFLOWNODE            |
| Resource Categories       | verify access rights (Edit) | RESOURCE_NODE               |
| Task Escalation           | verify access rights (Edit) | TASK_ESCALATION_NODE        |
| Task Templates            | verify access rights (Edit) | SCHEDULERTEMPLATETASK       |
| Task Workflow             | verify access rights (Edit) | TASKWORKFLOWNODE            |
| Time Sheet Coefficient    | verify access rights (Edit) | TIMESHEETCOEFFICIENTNODE    |
| Advanced Time Sheet Type  | verify access rights (Edit) | SCHEDREPORTTYPENODE         |
| Type of Work on Context   | verify access rights (Edit) | TYPEOFWORK                  |
| Type of Work              | verify access rights (Edit) | TYPEOFWORK                  |
| Request Tracking Accounts | verify access rights (Edit) | REQUESTTRACKINGNODE         |
| Severity                  | verify access rights (Edit) | SLASETTINGSNODE             |
| Service Level Agreement   | verify access rights (Edit) | SLASETTINGSNODE             |
| Service Hours             | verify access rights (Edit) | SLASETTINGSNODE             |
| Product Price List        | verify access rights (Edit) | ITEMPRICINGNODE             |

| Settings Option                       | Who can see                 | What node is checked   |
|---------------------------------------|-----------------------------|------------------------|
| Item                                  | verify access rights (Edit) | PRODUCTSETTINGSNODE    |
| Applications Settings                 | verify access rights (Edit) | USERPROFILENODE        |
| Form Manager                          | verify access rights (Edit) | FORMADMINNODE          |
| Education Levels                      | show to Admin only          | EDUCATIONLEVELSNODE    |
| Education Fields                      | show to Admin only          | EDUCATIONFIELDSNODE    |
| Education Subfields                   | show to Admin only          | EDUCATIONSUBFIELDSNODE |
| Document Types, Categories & Location | verify access rights (Edit) | DOCCATEGORYNODE        |
| Manage Print Templates                | verify access rights (Edit) | DOCCATEGORYNODE        |

# Groups & Roles

## About

Groups & Roles is utility that allows you to create **Groups** (or Roles) of users. This functionality works mainly to set-up system access rights. Using groups, you assign access rights to users in that group. Once you assign right to the (Access) Group, all users in that group will receive the same rights immediately. That is different from Roles. Access rights of users in Role(s) is not given to the users until they are assigned the Role on each individual Project, Folder or Activity. Assigning User to Role means they are allowed to occupy that particular Role.



## User Roles

## Video Tutorial on Roles

<https://www.youtube.com/embed/MyXIJ8OTnYY>

# User Profiles

**User Profiles** set Atollon **user interface** to default state, in which it reflect needs of user's **organization role**.

Each Profile may be associated with one application **Preset**. Each Atollon application may have one or more Presets. Preset holds any settings that are needed to customize Atollon to the need of your organization or your organization's role.

By combining User Profiles and Application Presets you may create unique set-ups of user interfaces, which is helpful when adjusting new organization roles.

## Create New User Profile

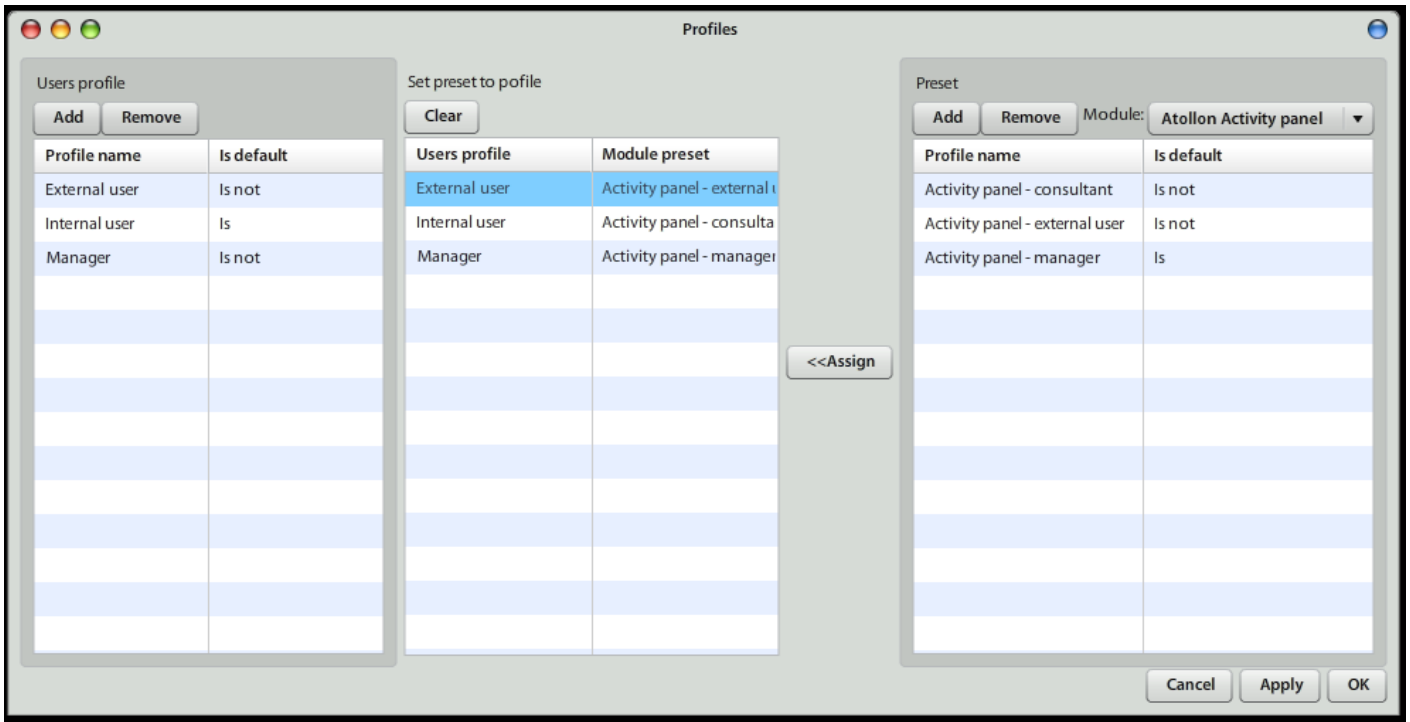
In order to create new User Profile, you may press on "Add" above Users Profiles table and press on Save. One of the User Profiles may become Default. Default is used once the user would not have assigned any profile.

## Create New Application Preset

In order to create Application Preset, select the Module on right (for example Activity Panel) and click on Add, give the new record some name and press Save. One of the Application Presets may be set as default. This Preset is used when no one is assigned to User Profile.

## Match Preset to Profile

You may set Application Preset to User Profile by selecting both records: Preset on right and Profile on left and pressing Assing. This way Atollon User, who has the User Profile will get the Application Preset.

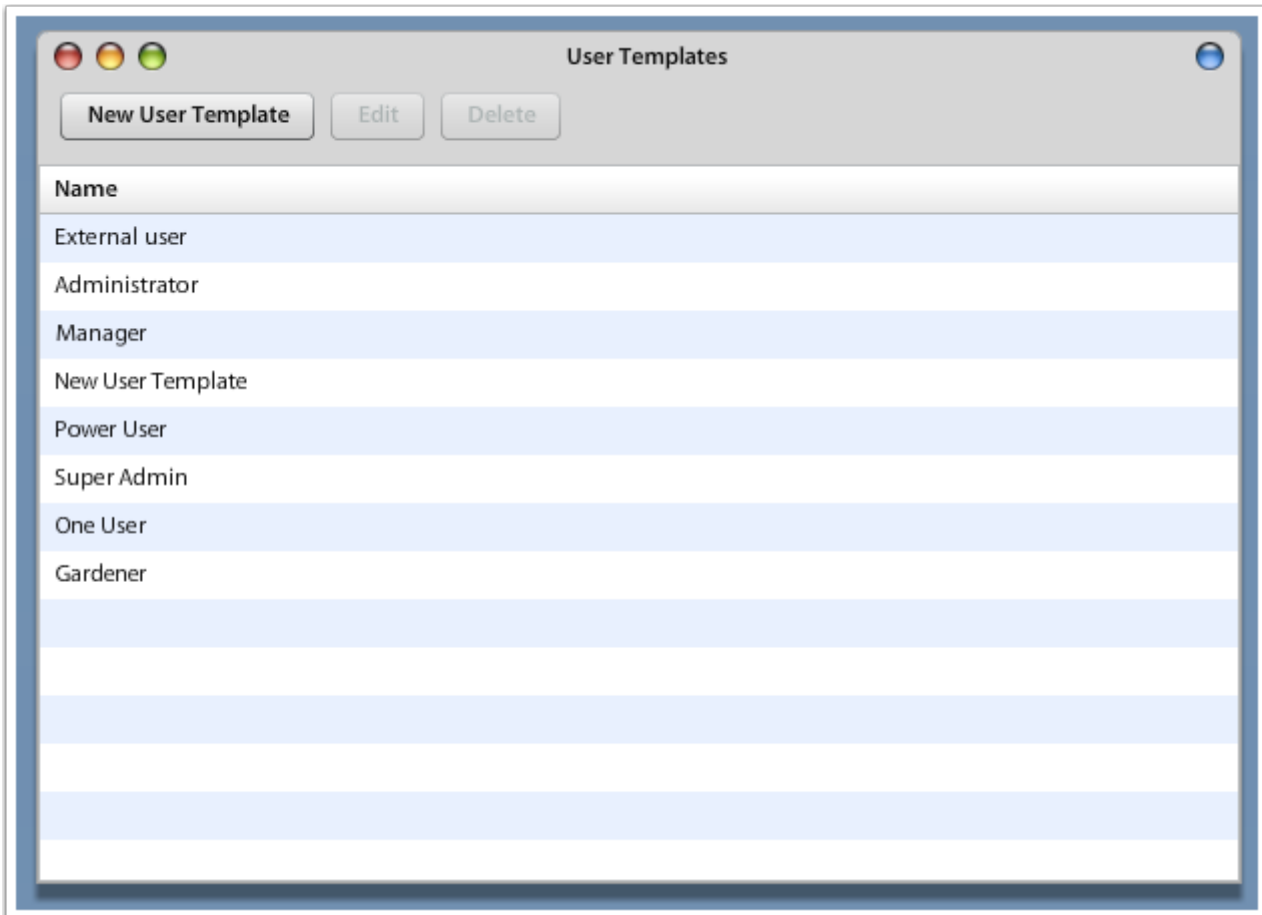


## Example

You may want to hide/show some tabs on Client's detail. This is accomplished using Activity Panels. Each type of Folder (Client, Prospect, ...) may have one or more definitions of what Tabs will be displayed for each particular organization role (ie Sales, Management, Service, ...). You may create as many Activity Panels as you want and store the mapping of Activity Panel to Folder Type into Application Preset. This Preset then may be assigned to User's Profile.

# User Templates

User Templates allow you predefine newly created User's settings. Change in User template does not have any effect on users that were created based on the selected template, they are just helpful when creating new users (so you don't have to reinvent the wheel all the time you need to create new user(s)).



## New User Template

The New User Template has all the same attributes that has New User. Please refer to [Users](#) documentation for more details.

