Unchained Role and Permission System

The Roles and Permissions Module provides the ability to limit system access and data access. We have two types of permissions available: Roles, and Permissions. Role level security provides access to features or modules with a simple yes/no access level. (For example, Does this User play a Role in the Ticket System in this Organization?). Permission level access is more granular, requiring a Role and a Permission record. A permission record is composed of R(ead), W(rite), U(pdate), D(elete) giving the system the ability to allow some roles to View data and other roles to View and Update data on certain specific object chains (object chains being similar to a database table).

Base Terminology

An Organization is a company that uses one or more federated servers (think Corporate Office XYZ and all of their branches). If your company launches multiple federated servers, it is recommended that you maintain ONE organization. This gives you accurate hierarchical accounting, and the ability to manage your organization more efficiently (think of centralized maintenance).

A User is a person who uses the system.

A Role is a record that allows a User to access a set of modules.

A User-Role is one access layer for a specific user and a specific role into the underlying data for a specific chain. A user may play multiple roles. A user may play multiple roles and also have multiple role permissions.

Step by Step Guide - How to start a new Organization

Click on Admin | Add Organization
Establish a BiblePay keypair for your organization (this allows your org to pay the hosting fees incurred when updating chain data). Be sure to back up the public and private keys as it is important to maintain the private key for the ability to back up your server data (if the private key is lost, you lose access to your data, your users, your posts, and all of the data, and no one can recover it).
Paste the Public key in the field.
Name the organization and fill out any additional domain fields, click Save.
Once your organization is saved, the entire system will rely on this Organization.ID for the Roles.
New orgs will need two organization level roles, one for ban management and one for tickets.
To do this, click Admin | Add Role.

Choose your new organization from the DropDown. For the role name, type “Superuser” (case sensitive) and click Save.
Then leave your organization selected and type “Ticket” (case sensitive) and click Save.
Ensure any administrative users who will use the system already exist as users and their e-mail addresses are verified before moving to the next step.

How do I Promote one (or more) Key individual(s) to Superuser?

Promote one of your key individuals to Superuser next (this will allow that user to promote others and perform management).
To do this click Admin | Organization Actions | Click the wrench next to your Organization.
From the Role Editor page, in Add User Role, choose the user from the User drop down that you wish to promote to superuser.
Next, change the Role name to Superuser for your Organization. NOTE: Do Not choose roles from other orgs, such as ‘system’ as that will not work.
For example, if your org is named XYZ, choose “XYZ – Superuser”.
Click Save User Role.
Now you have a person who is a superuser. This superuser has the ability to provide power roles to other users, or perform ban management.
(Optionally, if you want this person to have access to the ticket system, repeat the above procedure, and add a role named “XYZ -Ticket” to this user in the Add User Role section.

How do I perform Ban Management

As a superuser click on Admin | Ban Management.
Users have the ability to flag content as inappropriate. They can flag a video, a comment, a prayer, a townhall comment, or a timeline post as Inappropriate (by clicking the Ban icon next to parent items in the system).
Once this content is flagged, it goes into the Ban Management report, which shows Who reported it, Who originally posted it, and a URL column which is clickable, opening a new window that shows the original reported post in the original context.
In the case of a Comment, it will be highlighted in Yellow, but if a timeline post it will be by itself.
For the Ban Manager, the idea is to decide if you want the content to stay or go.
While reviewing each row on the report, click each URL link and review the content. If you allow it, switch windows back to the report, and click the Allow button for that row.
Once you allow content, we remove the item from the report and stamp the Ban record with the approver and the datetime.
If you click Remove, we will remove the content (make it unavailable to the web site) by updating it, making it no longer visible to your users. Then the ban record is updated and the item will be purged from the report.