Registration

Registration Fields

1. First log in to the administrative backend
2. Once logged in, find **Users** in the main menu bar located toward the top of the page.
3. Choose **Members** from the drop down menu
4. Click on the **Registration** tab
5. You should now be presented with a table of available user fields and their status for a particular action. This controls what fields the user will see, must fill in (required) or can fill in (optional) depending upon which action or state they are currently in. That is, you can make the username field required for the registration page (**create** column) but may not wish for your users to be able to edit this after creation (**read only** for the **update** and **edit** columns).
    - **Create column:** What the user sees on the registration page
    - **Proxy column:** What columns an administrator sees or must fill in when creating an account by proxy (i.e., for someone else)
    - **Update column:** What fields the user will see and/or must fill in if something has changed with what information is required at registration. An example of this would be if the **citizenship** field was, at one point, optional for registration but is now required. Setting this field to **Required** for the **Update** column will now require logged-in users to fill this information out.
    - **Edit column:** What fields the user will see and can edit for their user profile
    - **Field Option Definitions:**
        - **??**Required = Must fill in
        - Optional = Can fill in, but are not required
        - Hide = Not visible
        - Read only = Can view but cannot change
6. Once you feel ready to save your changes, scroll back to the top of the page and click **Save** in the upper right portion of the page. Changes take affect immediately.

Customizing Confirmation Email

All component layouts can be customized through overrides. Except for files that are provided in the Joomla! distribution itself, this method for customization eliminate the need for designers and developers to **hack** core files that could change when the site is updated to a new version. Because they are contained within the template, they can be deployed to the Web site without having to worry about changes being accidentally

User Authentication Plugins

A Hub can offer multiple ways for users to login through other services like LinkedIn, Facebook, ORCID, etc.

- Authentication-Certificate: Handles user authentication against client side SSL certificates
- Authentication-Facebook: Handles user authentication against Facebook
- Authentication-Google: Handles user authentication against Google
- Authentication-Hubzero: Default user authentication
- Authentication-LinkedIn: Handles user authentication against LinkedIn
- Authentication-ORCID: Handles user authentication against ORCID
- Authentication-Picas: Handles user authentication against Purdue's CAS
- Authentication-Twitter: Handles user authentication against Twitter

To activate these authentication plugins acquire a customer secret and customer key from the other service by registering your App on the service and selecting the Web format. Once you have the keys you can enable the plugins from the backend of the Hub.

1. Navigate to the backend of the Hub and locate the **Extensions Tab** and click on **Plug-in Manager**
2. Inside of the **Plug-in Manager**, search for the authentication plugin
3. Click on the title of the plugin and inside the plugin insert the **customer secret** and **customer key**
4. Change the *Status* of the plugin to **Enabled** and then click **Save & Close**

TLS Certificate Authentication

Certificate Authentication Plugin:

This plugin is in charge of actually checking the certificate and creating new accounts or linking [illegible] system). This plugin is called: Authentication - Certificate.

Enable the Authentication - Certificate Plugin:

1. Navigate to the backend of the Hub and locate the **Extensions** tab
2. Click on the **Extensions** tab and from the drop-down click on the **Plug-in Manager**
3. Locate from the plugin list or through search the **Authentication - Certificate** plugin
4. Click on the title of the plugin then locate the *Status* section inside the plugin
5. From the *Status* drop-down, select **Enabled** then click **Save & Close**

Certificate routing plugin:

This plugin handles the requirement for a certificate to be present while browsing the site. While the authentication plugin is what checks and links the user to the cert, other authentication could still be allowed. With this plugin enabled, a certificate must be present and authentication options are limited to just certificate based authentication. This plugin is called: System - Certificate.

Enable the System - Certificate plugin by following the same steps listed out above.

New account approval:

This allows admins to require approval of new accounts prior to their being able to access the site. When this is enabled, accounts pending approval can be found in the users manager on the backend. You can also elect to turn on an administrative dashboard module that lists accounts pending approval. And in the users manager parameters, you can enable administrator notifications to receive an email when new accounts are created. This allows the certificate->user link to be user initiated (rather than admin initiated), but still gated and admin approved.

In terms of apache configuration, **SSLVerifyClient optional** should be set. This will allow the certificate to be included, but also allow the CMS to handle the requirement for the certificate through the use of the certificate routing plugin mentioned above.
SSLOptions +StdEnvVars should also be set, as I'm sure it already is for you all. Lastly, make sure the site is forced to SSL via the Joomla global configuration on the backend.

Note: In order for this feature to be useful, all users need to gain a TLS Certificate and have it implemented in their browser prior to utilizing this authentication process.