# BrightSpace Copyright App

## How to Install

* Copy code to the appropriate directory in a LAMP stack
* Create a MySQL Database

CREATE TABLE

notifications

(

d2lusername VARCHAR(50) NOT NULL,

dateapproved DATETIME NOT NULL,

noticetype INT(2) NOT NULL,

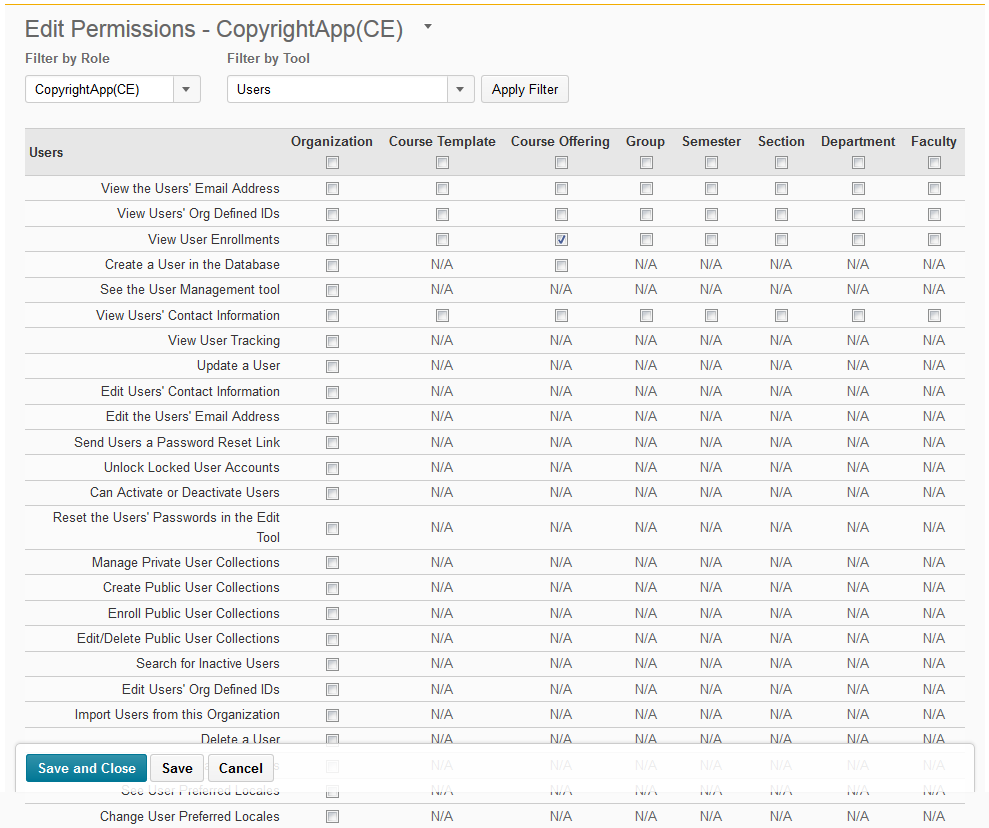
id bigint NOT NULL AUTO\_INCREMENT,

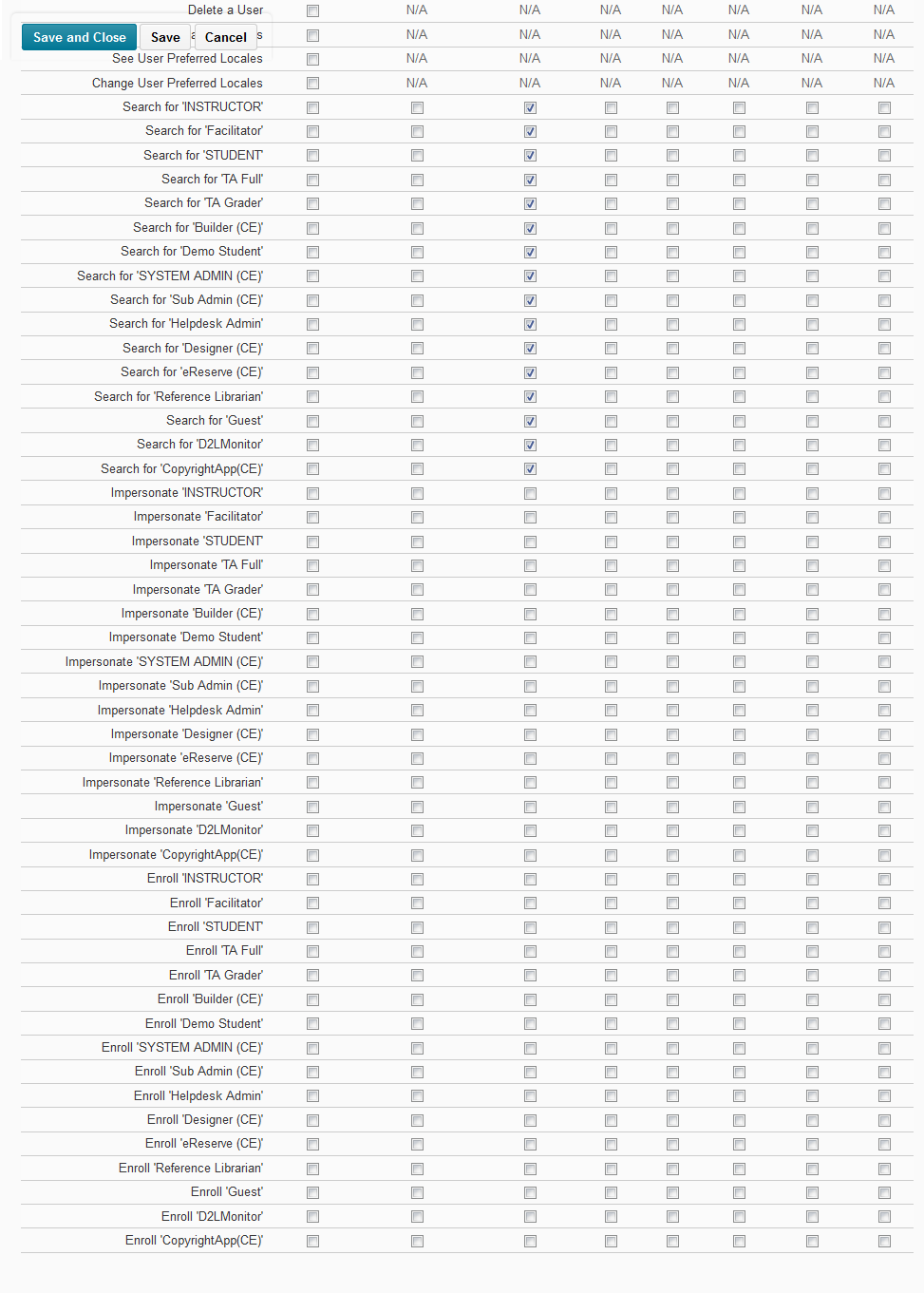
PRIMARY KEY (id)

)

ENGINE=MyISAM DEFAULT CHARSET=latin1;

* Update database information in config.php
* Login to BrightSpace as a System Admin
  + Cog -> Manage Extensibility -> Register an App
    - Application Name = Copyright Acknowledgement
  + Trusted URL = URL\_TO\_YOUR\_PHP\_SCRIPT // eg. https://util.library.dal.ca/brightspace-copyright-app/notice.php
  + Update config.php
    - APP\_ID = VALUE\_OF\_APP\_ID
    - APP\_KEY = VALUE\_OF\_APP\_KEY
  + Cog -> Roles & Permissions
  + Create a Role for copyright app eg. CopyrightApp
    - Give role the following permissions





* + Cog -> Users
    - Create a user specifically for the copyright app to access
    - Assign User the Role CopyrightApp
* Now, the next part is kind of hackey….
  + In a browser go to <https://apitesttool.desire2learnvalence.com/index.php>
  + Host = your brightspace url
  + Port = 443 (or may be different)
  + App ID = your app id you created in a previous step
  + App Key = your app key you created in a previous step
  + DO NOT PRESS AUTHENTICATE YET
  + In a new browser window login to BrightSpace
    - Cog-> Manage Extensibility
      * Click on your “Copyright Acknowledgement” Application you created previously
      * Click Edit
      * Change the Trusted URL to <https://apitesttool.desire2learnvalence.com/index.php>
      * Click Update
    - Cog -> Users
      * Find your copyright user
      * Impersonate your copyright user
  + Go back to the browser with the API Test Tool
    - Now Click “Authenticate”
    - You will now see a User ID and User Key
  + Update BrightSpace Info in config.php
    - USER\_ID = YOUR\_USER\_ID (from previous step)
    - USER\_KEY = YOUR\_USER\_KEY (from previous step)
  + Go back to BrightSpace and login as your Sys Admin user again
    - Cog-> Manage Extensibility
      * Click on your “Copyright Acknowledgement” Application you created previously
      * Click Edit
      * Change the Trusted URL back to your original value
      * Click Update
* Decide which Roles you want to view the pop-up
  + In BrightSpace, Cog->Roles & Permissions
  + Get the RoleId for a role by opening the Edit Role Screen. The URL will have the text roleId=### (### = some number) the ### is the Role ID number.
  + In config.php add your role id’s to the faculty $faculty\_groups array
* Open the file widgetcode.js
  + Enter the location of your php application with the server included. Eg. util.library.dal.ca/brightspace-copyright-app
  + Modify the “HTML CODE TO BE DISPLAYED IN POP-UP” section to the content you are looking for.
* Install the script in BrightSpace
  + Login to BrightSpace
  + Create new widget or modify existing widget
  + In the Widget Content Tab change to “HTML Source Editor” View
  + Copy the entire content of the file widgetcode.js and paste it into the text box for “HTML Source Editor”
  + Save Widget
  + If the widget does not already exist on your page, add it.

## Testing

* To test your user must be an instructor in a course, not just an instructor at the organization level.

## Notes

* http://docs.valence.desire2learn.com/basic/auth.html

**Users**. The application retrieves the User ID and Key indirectly during the authentication process in a browser or web-control. This model follows the one used in common web services (particularly, the three-legged model of OAuth). The user must separately authenticate with the LMS service, and must confirm granting access to the third-party application.

Additionally, after authentication, the granted User ID/Key pair is unique to the Application context (that is one Application ID cannot use the User ID and Key provided to another Application ID), and the requesting application can store the User ID/Key pair for long periods (by default, 30 days) because the Key is never directly exchanged during operations (instead, it uses the Key to craft signatures).

**Administrator or User on a compromised account**. In the event of a User Key becoming compromised (for instance, by losing a laptop or mobile device), both users and administrators can revoke tokens. If a user resets his or her password on the supporting back-end service, this will automatically revoke the privileges afforded any existing long-lived tokens generated for that user context: subsequent access by applications attempting to use that User ID/Key pair will fail, and the applications will need to have their controlling users re-authenticate with the service.

By default, the LMS service will maintain a provided User ID/Key pair as valid indefinitely; Administrators that want to revise this to a real time constraint (for example, 30 days) can contact their dedicated customer support contact.