v4 Security Hardening and Enhancements

These are some of the security changes in v4 compared to v3 to take note of:

1. Security Enhanced Directory Manager - New Security Enhanced Directory Manager is now available to provide enhanced security policies and features.
   This plugin can selected through the Directory Manager Settings.
   Note that once this is enabled, all user passwords will be stored using stronger encryption, so you cannot switch back to the default Directory Manager as users would no longer be able to login.
2. **Error Messages** - If an unexpected server error 500 occurs, the browser now only shows a generic message and the exceptions and stacktraces are logged in the log files.
3. **Passwords** - All passwords are no longer viewable in the HTML source.
4. **Default Process Start White List** - For newly deployed processes, the Process Start White List is set to the admin role by default.
5. **User Profile** - User profile update now requires authentication.
6. **User Creation** - If user is created by a non-admin user (e.g. in an app), that user is automatically assigned a normal user role.
7. **License Information** - License information in the web console footer is now only visible to administrators.
8. **Workflow Designer** - The workflow designer now supports prompting for password when the user session times out.
9. **Form Elements** - Labels and values do not allow script execution to prevent possible cross-site scripting (XSS) vulnerabilities.
10. **Readonly Form Elements** - Read-only field values are no longer stored upon form submission to prevent unintended modifications using client-side browser tools such as Browser Console, Firebug, etc.
11. **JSON API Requests** - JSON API requests that modify state now only accept HTTP POST only to prevent cross-site request forgery (CSRF).
12. **JSON API Authentication** - JSON API now supports HTTP basic authentication.
13. **JavaScript API Authentication** - JavaScript API AssignmentManager.loginWithHash call introduced to accept login with user hash.