



Great Ideas. Always Flowing.™

Dynamic Login 4.1

User Guide

Table of contents:

1	INTRODUCTION	4
1.1	What's new in 4.1.....	5
2	INSTALLATION PROCEDURE.....	6
3	ADDING DYNAMIC LOGIN MODULE TO A PAGE	10
4	MAKING YOUR DYNAMIC LOGIN MODULE/PAGE THE MAIN LOGIN PAGE OF THE SITE 12	
5	DYNAMIC LOGIN MAIN MENU	14
5.1	Entering the product license and registering the module	15
5.2	Initial layout and suggested sequence of setting the Dynamic Login	17
6	USING THE CONTROL PANEL	18
7	MANAGING THE TEMPLATE	19
8	MANAGING ROLE RULES	22
8.1	Adding a new Rule Role.....	24
8.1.1	Managing existing links.....	25
8.2	Editing an existing role rule	26
9	MANAGING SECURITY ROLE GROUP RULES	27
9.1	Adding a New Role Group Rule	28
10	MANAGING USER NOTIFICATIONS	30
11	RESTRICTING BY IP/SQL VALIDATION.....	32
11.1	Restricting Login by IP access.....	33
11.1.1	Blocking an IP address.....	33
11.2	Restricting Login by SQL validation.....	34
12	MANAGING SINGLE SIGN ON	35
13	MANAGING MODULE CONFIGURATION	37
13.1	Managing the General Settings.....	38
13.2	Setting the Button Type.....	40
13.3	Forcing Profile Change/Password Update Pages.....	41
13.4	Managing the Login Template Stylesheet.....	42
13.5	Executing an SQL Query	43
13.6	Facebook Connect Integration.....	43
13.6.1	Managing General Facebook Connect Settings	44
13.6.1.1	Managing Facebook Wall Post Settings	47
13.6.1.2	Facebook Connect from your Users' Perspective	48
13.7	Setting up the Twitter Connect Integration.....	50
13.8	Setting up the Linked in Connect Integration	51
14	AUTO SIGN-IN FEATURE	52
14.1	Instructions for setting up Auto Sign in	52
15	DROPDOWN LOGIN INTEGRATION SKIN OBJECT	53
15.1	Instructions on implementing this feature.....	53
16	DELETING DYNAMIC LOGIN MODULE.....	54

List of figures:

Figure 1:	Installation procedure (step 1/9)	6
Figure 2:	Installation procedure (step 2/9)	6
Figure 3:	Installation procedure (step 3/9)	6
Figure 4:	Installation procedure (step 4/9)	7
Figure 5:	Installation procedure (step 5/9)	7
Figure 6:	Installation procedure (step 6/9)	8
Figure 7:	Installation procedure (step 7/9)	8
Figure 8:	Installation procedure (step 8/9)	8
Figure 9:	Installation procedure (step 9/9)	9
Figure 10:	Adding a module to a page.....	10
Figure 11:	Dynamic Login module added to the page	11
Figure 12:	Making the Dynamic Login the main site login page (step 1/)	12
Figure 13:	Making the Dynamic Login the main site login page (step 2/)	12
Figure 14:	Setting the page security to "Administrators only"	13
Figure 15:	Opening the main menu	14
Figure 16:	Entering the product license and registering the module (step 1/2)	15
Figure 17:	Entering the product license and registering the module (step 2/2)	16

Figure 18: Initial layout and setup	17
Figure 19: Using the control panel (step 1/2)	18
Figure 20: Using the control panel (step 2/2)	18
Figure 21: Managing the login template	19
Figure 22: Verification label and textbox.....	20
Figure 23: Demonstration of the form parameters.....	21
Figure 24: Demonstration of the form parameters.....	21
Figure 25: Demonstration of the Facebook Connect button.....	21
Figure 26: Choosing option "Security role rules"	22
Figure 27: Options available inside the edit role rules screen	22
Figure 28: Message displayed to the user after signing in	23
Figure 29: Adding a new Security Role	24
Figure 30: Choosing option "Select an Existing URL"	25
Figure 31: Managing existing links.....	25
Figure 32: Editing an existing role.....	26
Figure 33: Choosing the "Security Role Group Rules" option	27
Figure 34: Managing Role Group Rules	27
Figure 35: Adding a new group rule.....	28
Figure 36: Example of the role groups.....	29
Figure 37: Managing the user notifications.....	30
Figure 38: Managing the user notifications.....	30
Figure 39: User successfully added to the list	31
Figure 40: Restricting by IP/SQL validation	32
Figure 41: Restricting by IP and SQL validation	32
Figure 42: Blocking an IP address.....	33
Figure 43: Restricting Login by SQL validation.....	34
Figure 44: Managing Single Sign On	35
Figure 45: Choosing option "Module Configuration"	37
Figure 46: Choosing option "Dynamic Login Settings"	37
Figure 47: Managing the general settings	38
Figure 48: Setting the button type.....	40
Figure 49: Forcing Profile Change/Password Update Pages	41
Figure 50: Managing the Login Template Stylesheet	42
Figure 51: Executing an SQL Query	43
Figure 52: Available Facebook Connect options	43
Figure 53: Managing General Facebook Connect Settings.....	44
Figure 54: Managing Facebook Wall Post Settings.....	47
Figure 55: Facebook Connect as Seen by Your Users (1/4)	48
Figure 56: Facebook Connect as Seen by Your Users (2/4)	48
Figure 57: Facebook Connect as Seen by Your Users (3/4)	49
Figure 58: Facebook Connect as Seen by Your Users (4/4)	49
Figure 59: The way the wall post has been setup	49
Figure 60: Setting up the Twitter Connect Integration	50
Figure 61: Setting up the Linked in Connect Integration	51
Figure 62: Example 1	53
Figure 63: Example 2	53
Figure 64: Deleting Dynamic Login (step 1/2)	54
Figure 65: Deleting Dynamic Login (step 2/2)	54

1 INTRODUCTION

The “Dynamic Login” module allows administrators to customize their portal and offer additional features and enhancements during the login process such as:

- **Add ‘Dynamic Role Rules’** to redirect the user to different pages on your site based on their roles in the portal
- **Setup default forwarding to default users** to a particular page that’s not just the home page
- **Add notifications to the administrator** if a particular user signs in
- **Add message notifications to users/roles**, once they sign in the message can be displayed to the user/role
- Several extended and optional features to **enhance the overall portal login process**
- **No changes to DNN Core**, simply add module to a new page and change the login page under 'Site Settings', 'Login Page'.
- **Complete layout control** - Now you can setup a custom template for your login page. This means that if you don't want to include the register link at all, or maybe the 'Remember Me' or 'Send Password Reminder' links you could simply remove them from the template. Or you could easily change the labels, or look of the fields. For example let's say you want to put both the username textbox and password textbox on the same row? Each different implementation is different but the key here is that you have a full control of the login template using login [Tokens] that are then replaced at run time with specialized controls
- With new login tokens you can also choose to **use Login Image Buttons instead of links** buttons for your login page
- New feature to allow the user to be able to **sign in with their email address**
- New feature to allow the user to be able to **sign in with their UserID** (the number, separate from the username)
- New feature to **automatically bypass the role and user redirection rules** and redirect the user to the previous URL.
- New Single Sign On (SSO) functionality. This new enhancement allows for other portals within the DNN installation to be able to access the portal if the SSO feature is turned on and the user enters the login credentials correctly for the 'Master Portal'

1.1 What's new in 4.1

- **New Social Media Connect Integration**
 - **New Twitter Connect Integration** – Now allow users to login via their Twitter account. Optionally post a message to their Twitter account profile whenever they sign in via the Twitter Connect integration feature!
 - **New LinkedIn Connection Integration** – Now allow users to login via their LinkedIn Account. Optionally post a message to their LinkedIn account profile whenever they sign in via the LinkedIn integration feature!
 - **Updated Facebook Connect** – New features that fix new requirements for OAUTH 2.0 w/ Facebook
 - **Updated Facebook Connect** – New features to store the Facebook Authentication Token within a session variable (and option to then use it/store it within a user profile field)

2 INSTALLATION PROCEDURE

In order to install your “Dynamic Login 4.1” module, login with an account to your DNN site as a host or administrator account. Once you have logged in, choose **Extensions** from the **Host** menu”.

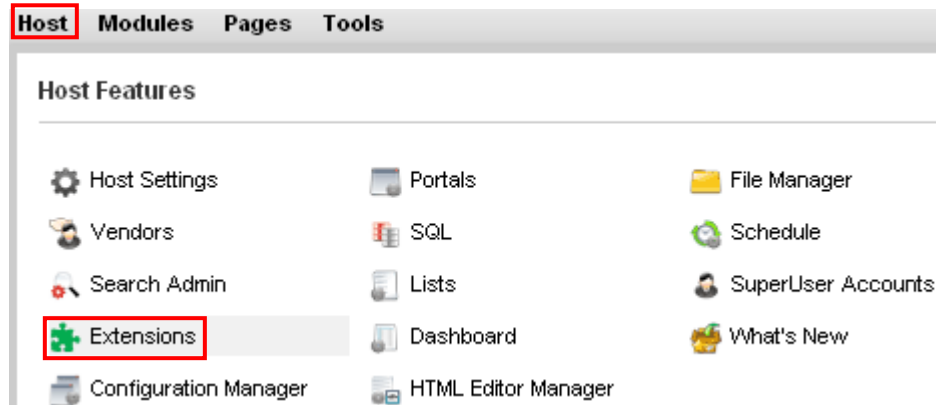


Figure 1: Installation procedure (step 1/9)

The following page will be displayed.

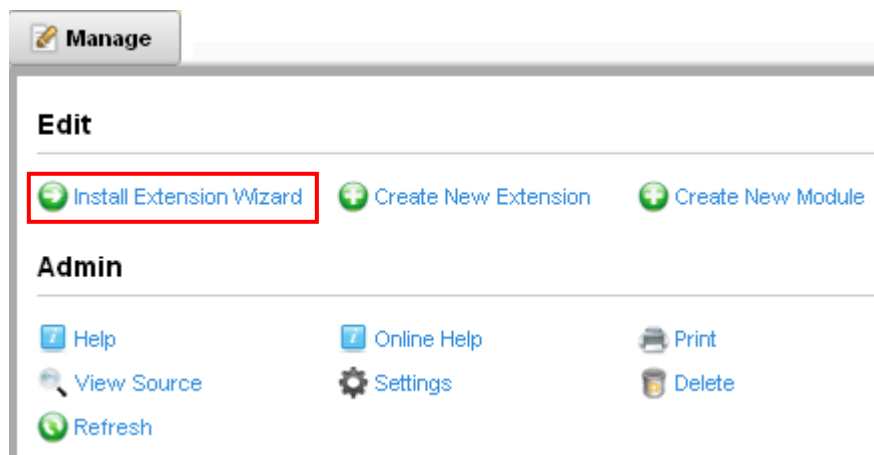


Figure 2: Installation procedure (step 2/9)

Click **Install Extension Wizard** to continue installing “Interactive User Import” and the following page will be displayed.

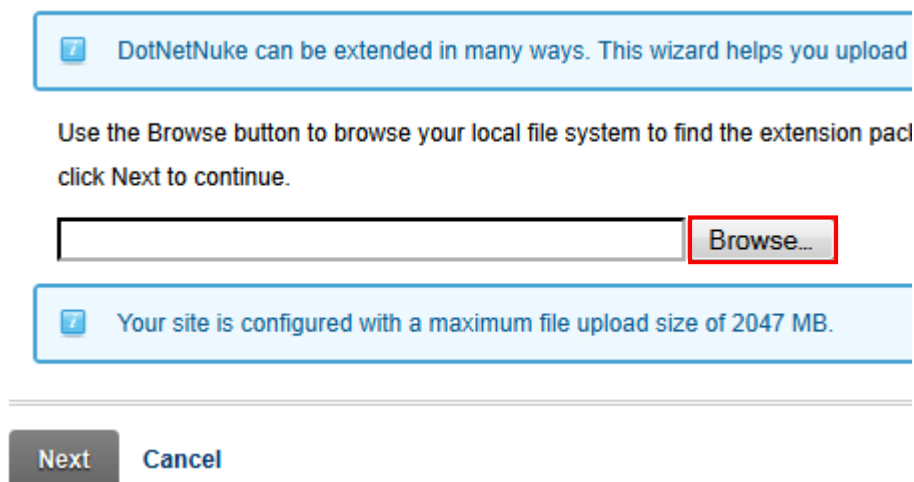


Figure 3: Installation procedure (step 3/9)

Click **Choose File** to locate the installation file on your PC.

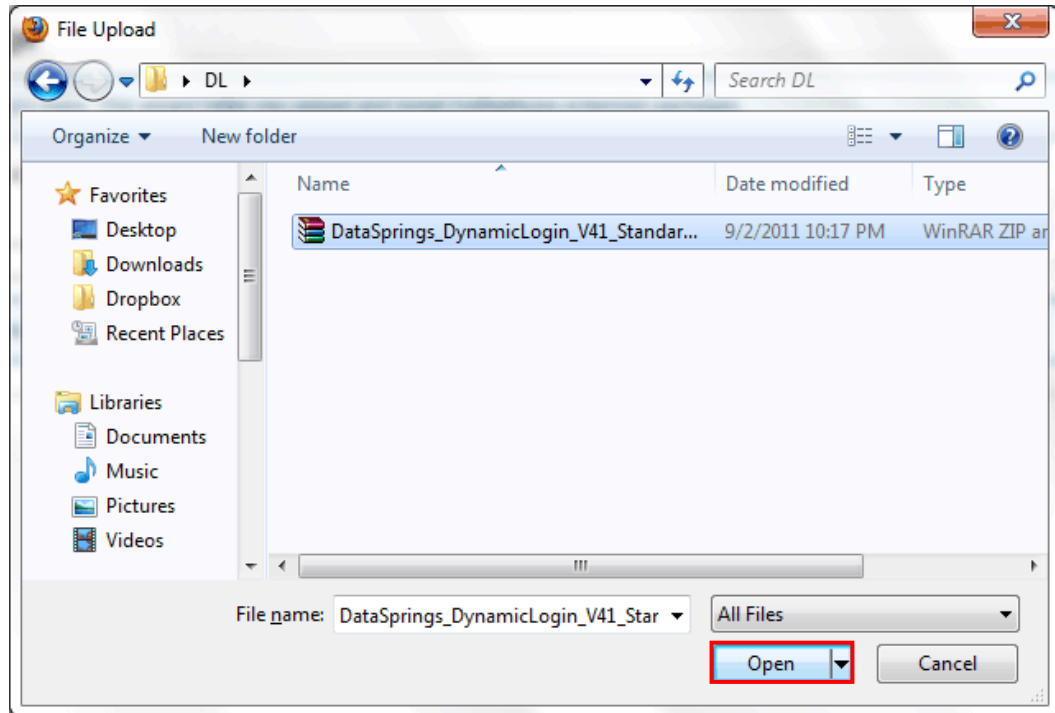


Figure 4: Installation procedure (step 4/9)

Locate the installation file and click **Open**. The following page will be displayed.

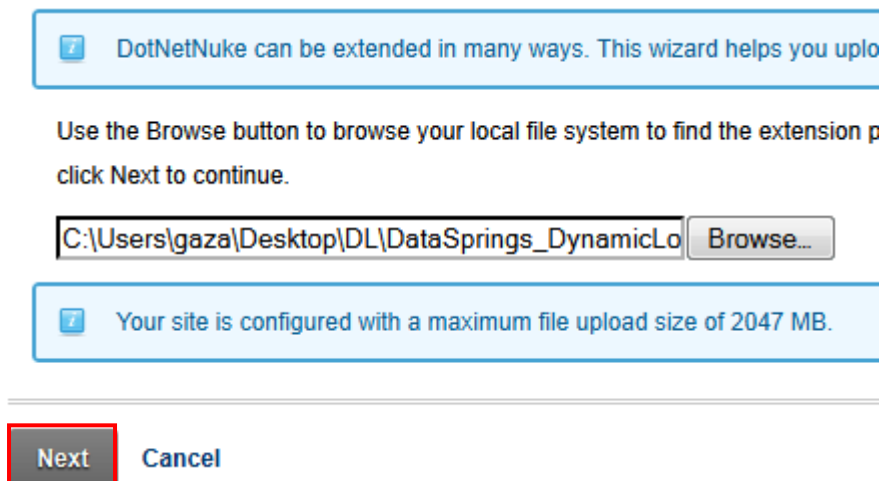












Figure 5: Installation procedure (step 5/9)

Click **Next** and the “Package Information” will be displayed.

Package Information

 The following information was found in the package manifest.

Name:  Dynamic Login
Type:  Module
Friendly Name:  Dynamic Login
Icon File: 
Description:  Tracks user activity and emails
Version:  4.0.20
Owner:  Data Springs, Inc
Organization:  Data Springs, Inc
Url:  www.datasprings.com
Email Address:  dnnsupport@datasprings.com

Next

Cancel

Figure 6: Installation procedure (step 6/9)

Click “Next” and the “Release Notes” page will be displayed.

Release Notes

 You can review the Release Notes for this package.

Release Notes:  The 4.0 release inc

Next

Cancel

Figure 7: Installation procedure (step 7/9)

Click “Next” and the “Review License” page will be displayed.

Accept License?  ☒

Next

Cancel

Figure 8: Installation procedure (step 8/9)

Select the "Accept License" to indicate that you accept the license and click **Next**. The installation will begin and after a couple of moments you will see the confirmation message in the bottom of the page.

Info Installation committed

Info Installation successful. - Dynamic Login

Info Deleted temporary install folder

EndJob Installation successful.

Return

Figure 9: Installation procedure (step 9/9)

Note: please keep track of any errors that appear during the installation. These errors can be helpful if your module has problems.

3 ADDING DYNAMIC LOGIN MODULE TO A PAGE

In order to add “Interactive User Import” module to a desired page follow these steps:

1. Select **Add New Module**
2. Choose **Interactive User Import** from the **Module** pull down menu
3. Click **Add Module**

The screenshot shows the 'Add Module' dialog box. The 'Add New Module' radio button is selected. The 'Module' dropdown menu is set to 'Dynamic Login'. The 'Add Module' button is at the bottom. The background shows a sidebar with 'Getting Started' and 'Our Services' sections, and a main content area with a 'YOU ARE HERE:' breadcrumb and a 'Dynamic Login' module preview.

Figure 10: Adding a module to a page

The “Dynamic Login” module will be added to the page.

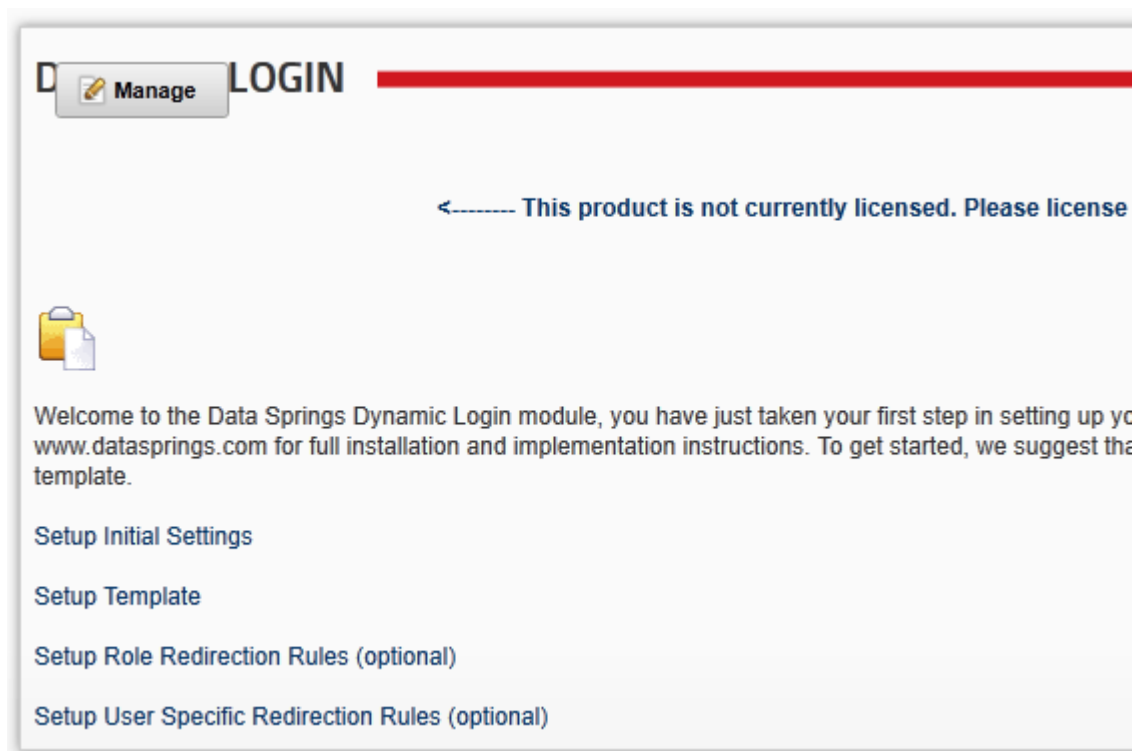


Figure 11: Dynamic Login module added to the page

4 MAKING YOUR DYNAMIC LOGIN MODULE/PAGE THE MAIN LOGIN PAGE OF THE SITE

IMPORTANT NOTE:

Before making Dynamic Login your primary login page, test it first to make sure that it is working properly.

If you cannot sign into Dynamic Login and have not configured the module properly, then when you setup your login page to be the Dynamic Login page you will have locked yourself out of the site.

If this does happen please contact support for assistance in updating your portals table to reflect a null value for the login page.

In order to make your Dynamic Login module/page the main login page of your site, you first need to choose the login page. In order to do so, click **Admin** and choose **Site Settings**.

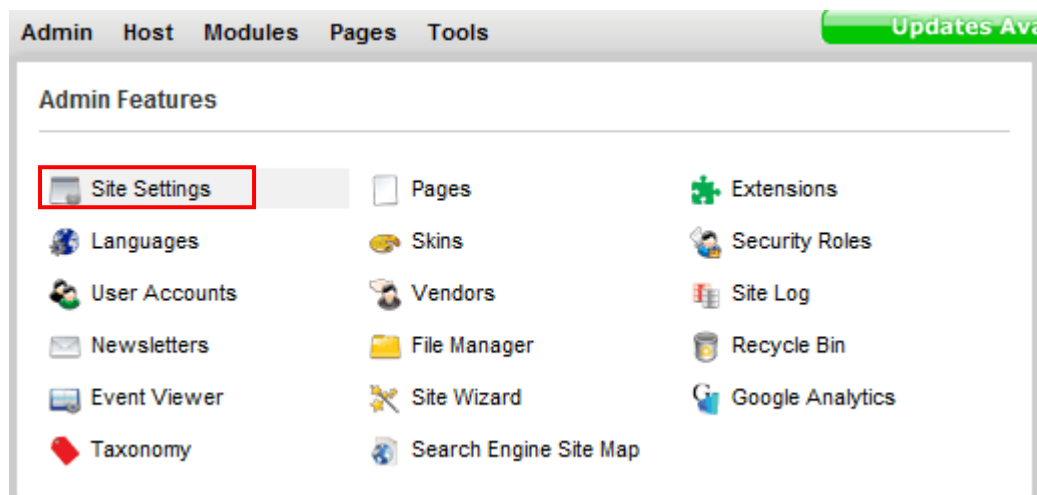


Figure 12: Making the Dynamic Login the main site login page (step 1/)

Within the **Settings** page, look under **Advanced Settings -> Page Management** and you will see the **Login Page** parameter.

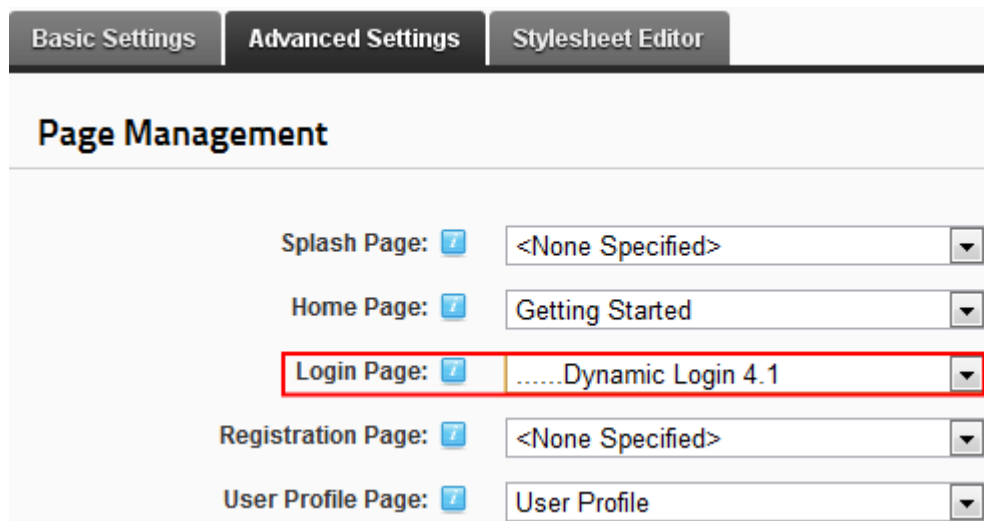


Figure 13: Making the Dynamic Login the main site login page (step 2/)

Choose the login page from the **Login Page** pull down menu.

Note: There is a feature that must be implemented starting in DNN 5.x. DNN included some code to force the standard account login module on the page and they did this because if your login isn't setup and working correctly you can never sign in.

So, in order for us to get around this DNN left a door open for modules such as Dynamic Login. Simply include an **Account Login** module on the page where the **Dynamic Login** module is specified and check the security to be 'Admin Only'.

So, first choose the **Settings** option from the main menu. Within the **Settings** page, select **Administrators** only.

Basic Settings

Module Culture: Neutral Culture

Module: Account Login

Module Title: Account Login

Tags:

Permissions:

Filter By Group: < Global Roles > ▼



	View Module	Edit Module
Administrators		
All Users	<input type="checkbox"/>	<input type="checkbox"/>
Candee's Test Users	<input type="checkbox"/>	<input type="checkbox"/>
Data Springs Blog Poster	<input type="checkbox"/>	<input type="checkbox"/>

Figure 14: Setting the page security to "Administrators only"

This way DNN can still recognize the Dynamic Login page as the main login page.

5 DYNAMIC LOGIN MAIN MENU

In order to start using the main menu, place your mouse over the “Dynamic Login” label and the **Manage** option will appear. Click **Manage** to open the menu.

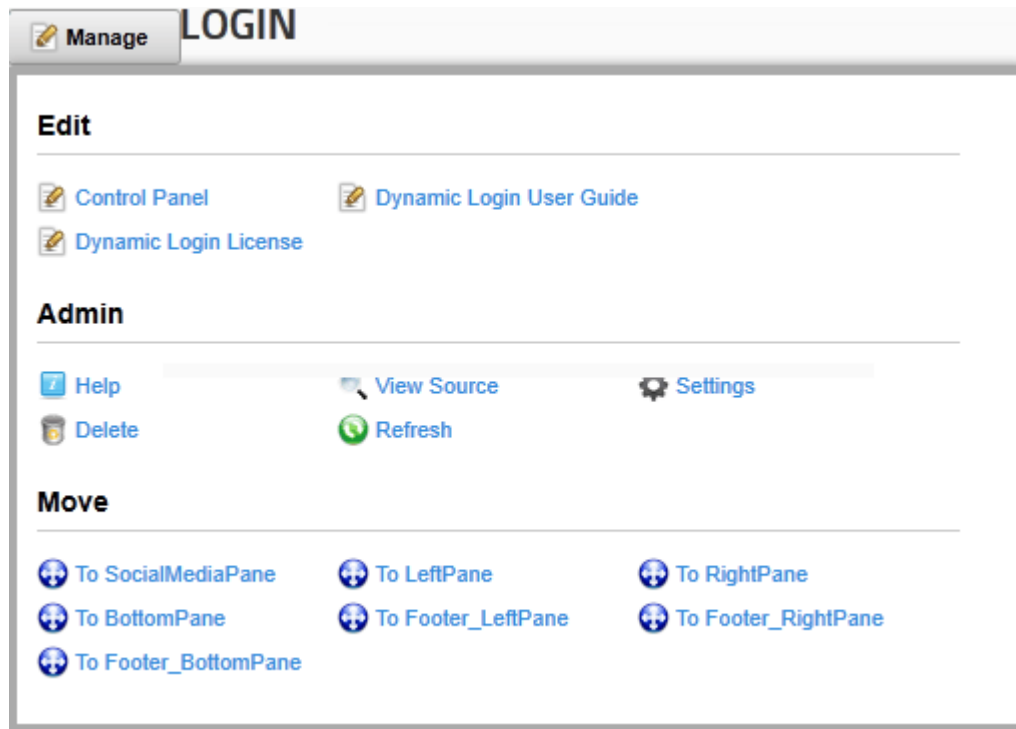


Figure 15: Opening the main menu

The following options are available inside this screen:

- **Control Panel** – the control panel with all major application options (see section 6)
- **Dynamic Login User Guide** – this guide
- **Dynamic Login License** – the option for registering the module (see section 5.1)
- **Settings** – option for managing settings (see section 13)
- **Delete** – option for deleting a module (see section 14)
- **Initial application layout** – see section 5.1

5.1 Entering the product license and registering the module

In order to register the module, you need to enter the module license, i.e. "Invoice ID". Choose option "Dynamic login License" from the main menu.

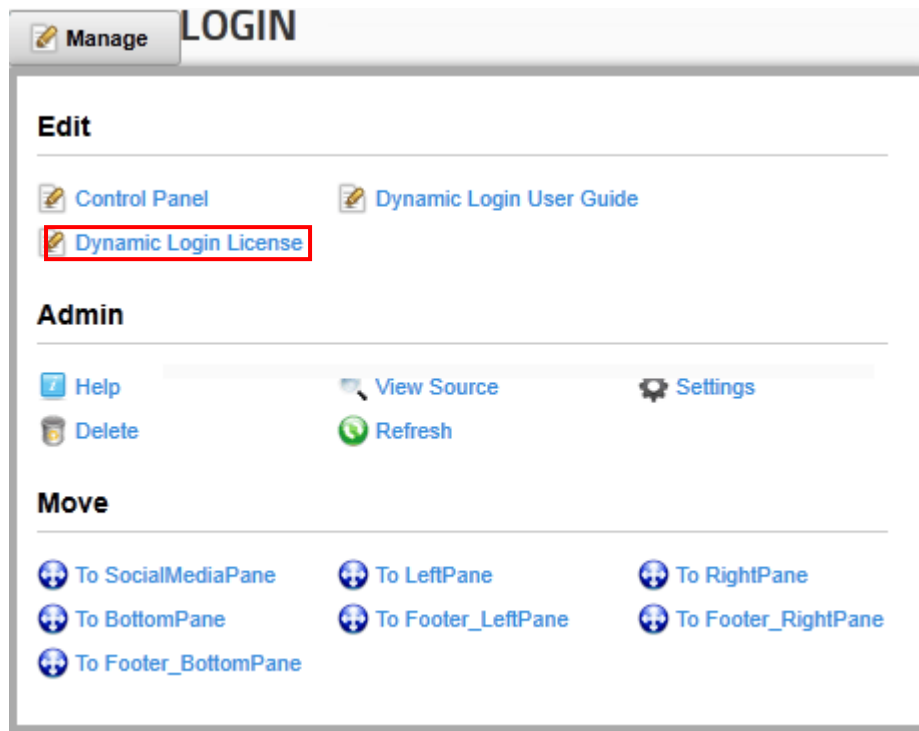


Figure 16: Entering the product license and registering the module (step 1/2)

The following page will be displayed.

YOU ARE HERE:

Module Training

Dynamic Forms Training

Dynamic Login 4.1

DATA SPRINGS PRODUCT LICENSING

DNN Version:	6.0.0
Product:	Dynamic Login
Product Variant:	Standard Edition
Product Version:	4.0.20.18587
Machine Key:	E8EBFF68-39EA-46B0-950A-CFD11D58FD0B
Host Title:	DotNetNuke
Portals:	My Website (training.betasprings.com)
IP Address:	89.216.213.151
Contact / Developer Name:	<input type="text" value="Chad Nash"/>
Contact / Developer Email:	<input type="text" value="cnash@datasprings.com"/>
Customer Name:	<input type="text" value="John Smith"/>
Invoice ID:	<input type="text"/>

☒ BY CHECKING THE BOX INDICATING I AGREE TO THE

[Register / Submit License](#) [Exit](#)

Figure 17: Entering the product license and registering the module (step 2/2)

Enter the license (received in an email after purchasing the product) under “Invoice ID” and click “Register/Submit License”. The module will be registered.

5.2 Initial layout and suggested sequence of setting the Dynamic Login

Initially the **Dynamic Login** interface contains additional options which are actually shortcuts to the options from the menu.

The purpose of placing these options/shortcuts here is to suggest the optimal sequence of actions you need to perform in order to setup your Dynamic Login application successfully.

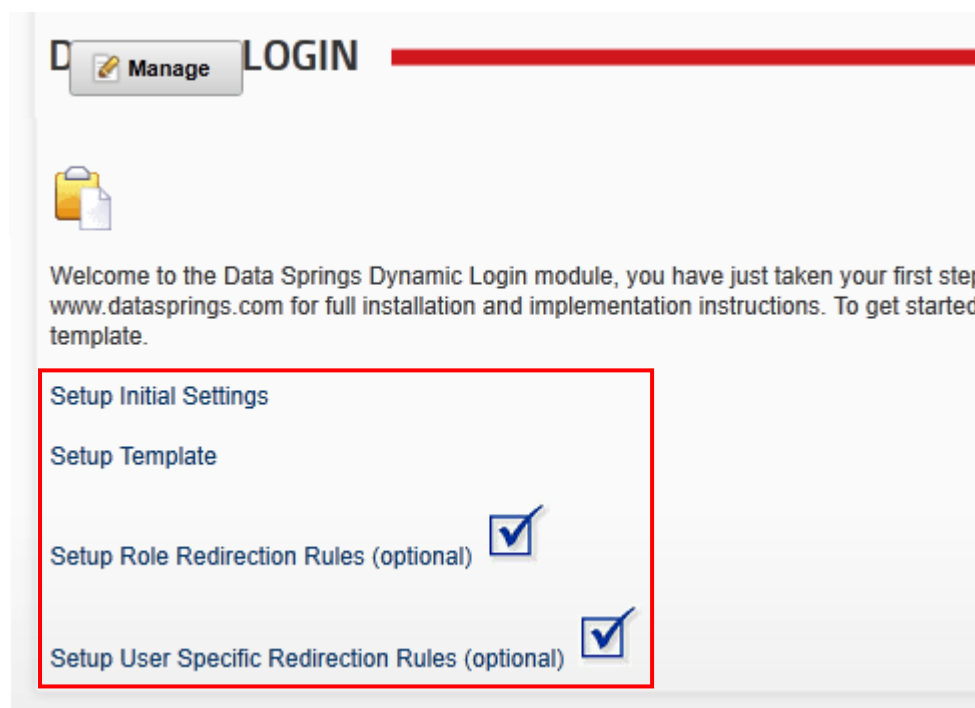


Figure 18: Initial layout and setup

The following options are available:

- **Setup Initial Settings** – see section 5.1
- **Setup Template** – see section 7
- **Setup Role Redirection Rules** – see section 8
- **Setup User Specific Redirection Rules** – see section 6

Once you complete the task successfully, this icon  will be displayed next to the option denoting the successful completion.

6 USING THE CONTROL PANEL

In order to start using the control panel, choose that option from the main menu.

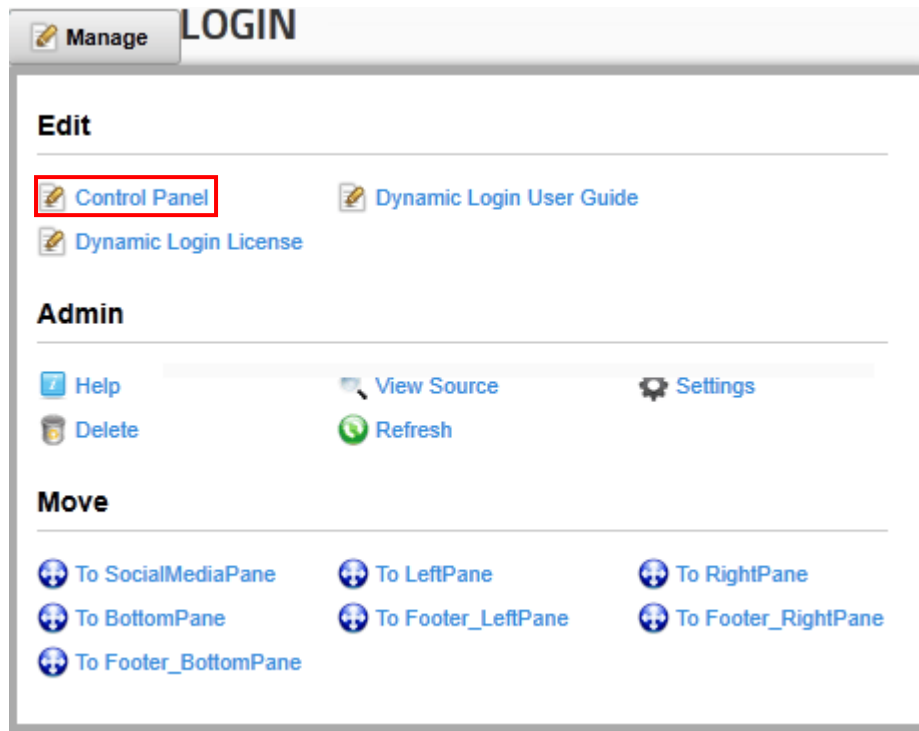


Figure 19: Using the control panel (step 1/2)

The following page will be displayed.



Figure 20: Using the control panel (step 2/2)

The following options and parameters are available:

- **Manage Template** – see section 7
- **Module Configuration** – see section 13
- **Security Role Rules** – see section 8
- **Security Role Group Rules** – see section 9
- **User Notifications** – see section 10
- **Restrict by IP/SQL Validation** – see section 11
- **Single Sign On** – see section 10

7 MANAGING THE TEMPLATE

The “Dynamic Login” module allows you to customize the layout of the login form. In order to start modifying the template, access the control panel (“Control Panel” option in the main menu) and the first page, displayed by default, is the page for managing the template.

You can access the page at any time while in control panel, by clicking the “Manage Template” option.

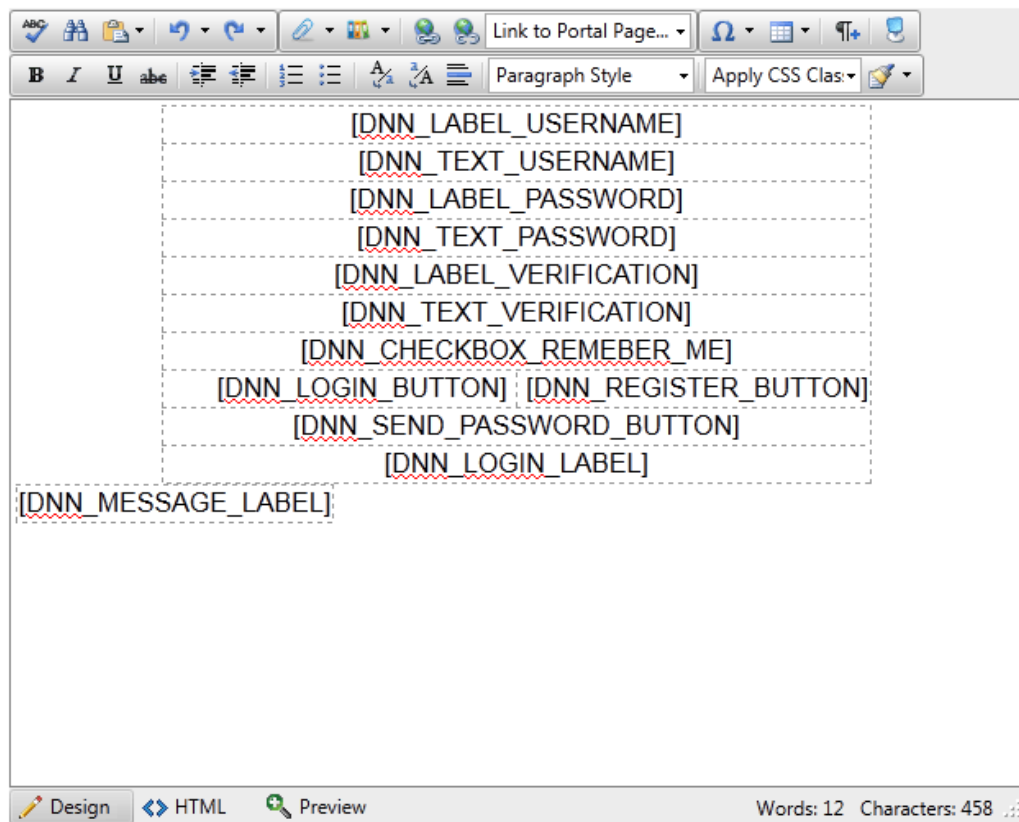
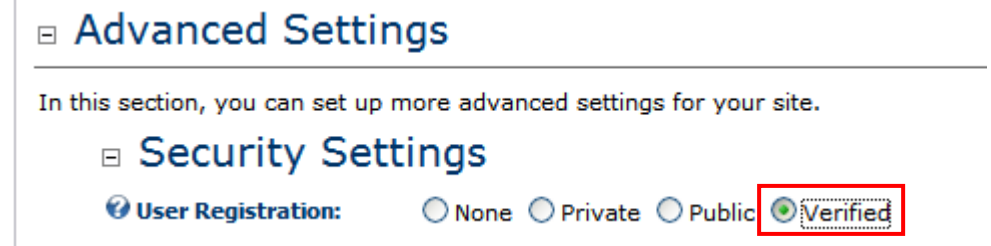


Figure 21: Managing the login template

The following parameters and options are available inside this screen:

- **Basic Text Box** – use this option only if you wish to have a very simple form
- **Rich Text Editor** – select if you want to use text formatting options
- **Text area** – this area is used for creating the template by using options inside the rich editor as well as the form parameters:
 - **[DNN_LABEL_USERNAME]** – use this parameter to determine the location of the “User name” label (see Figure 23)
 - **[DNN_TEXT_USERNAME]** – use this parameter to determine the location of the user name input field (see Figure 23)
 - **[DNN_LABEL_PASSWORD]** – use this parameter to determine the location of the “Password” label (see Figure 23)
 - **[DNN_TEXT_PASSWORD]** – use this parameter to determine the location of the password input field (see Figure 23)
 - **[DNN_LABEL_VERIFICATION]** – use this parameter to determine the location of the verification label. This label is displayed in case your registration is set to ‘Verified’ and the user is not verified (**note:** to turn verification on within DotNetNuke® go to Admin, Site Settings, Advanced Settings, and under Security Settings check the Verified radio button). The verification email will typically include

a verification code and/or a verification link to the login page which will pass along information to display the verification prompt.



This screenshot below demonstrates the label and textbox for verification when a user has not been verified and is attempting to sign in (or navigates to the verification link).

Figure 22: Verification label and textbox

- **[DNN_TEXT_VERIFICATION]** – the parameter for displaying the verification in put field input (see figure above)
- **[DNN_CHECKBOX_REMEMBER_ME]** – use this parameter to determine the location of the “Remember me” checkbox which will help your users login without the need for entering username and password each time (see Figure 24)
- **[DNN_LOGIN_BUTTON]** - use this parameter to determine the location of the “Login” button (see Figure 24)
- **[DNN_REGISTER_BUTTON]** - use this parameter to determine the location of the “Register” button (see Figure 24)
- **[DNN_SEND_PASSWORD_BUTTON]** - use this parameter to determine the location of the “Send password” button (see Figure 24)
- **[DNN_FACEBOOK]** – use this token to display the Facebook Connect button (see Figure 25)

Note: you may now login using your email address or your username.

User Name: [DNN_LABEL_USERNAME]

Password: [DNN_LABEL_PASSWORD]

☐ Remember Login

Not yet a member? Data Springs offers members premium site access to product forums, demonstrations, and resource sharing access within the site.

Want to customize your login module with a custom look and feel? Check out the latest version of [Dynamic Login](#).

Figure 23: Demonstration of the form parameters

Note: you may now login using your email address or your username.

User Name: [DNN_LABEL_USERNAME]

Password: [DNN_LABEL_PASSWORD]

☐ Remember Login [DNN_CHECKBOX_REMEMBER_ME]

[DNN_LOGIN_BUTTON] [DNN_REGISTER_BUTTON]

[DNN_SEND_PASSWORD_BUTTON]

Not yet a member? Data Springs offers members premium site access to product forums, demonstrations, and resource sharing access within the site.

Registration is free and easy! [Click here to Register](#).

Want to customize your login module with a custom look and feel? Check out the latest version of [Dynamic Login](#).

Figure 24: Demonstration of the form parameters

Quick login...

LOG IN

Or... now make it easy with Facebook Integration

[DNN_FACEBOOK]

Figure 25: Demonstration of the Facebook Connect button

After setting the desired parameters, click on the "Save" link in order to save the changes.

8 MANAGING ROLE RULES

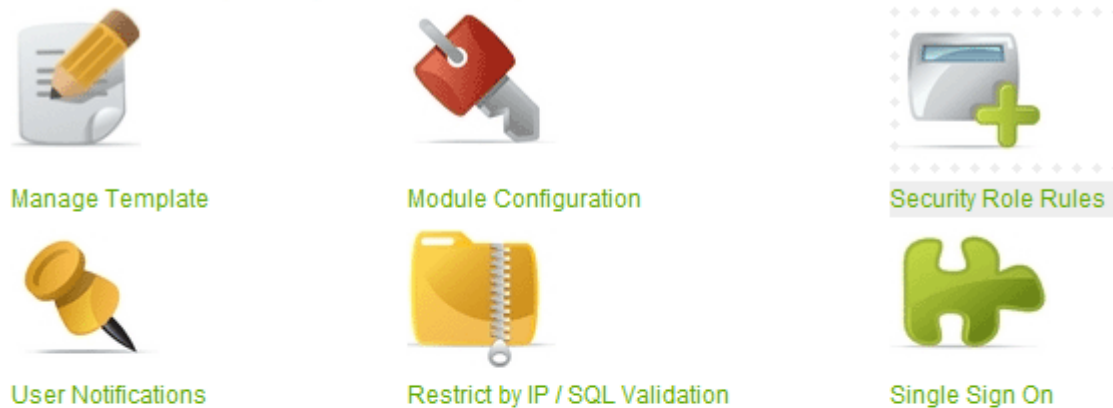
In order to start managing login rules based on user role in the system choose option "Security Role Rules" from the main menu.



Figure 26: Choosing option "Security role rules"

The following screen will be displayed.

Data Springs Dynamic Login Control Panel



Security Role Rules allow you to redirect the user or display unique messages to the user based on a host users and can be setup based on priority (higher priority number means a higher priority). Unique priority levels such as 100, 200, 300, etc...





Role Name	Url
 Registered Users	http://www.registeredusers.com
 Subscribers	http://www.registeredusers.com
 Role:	<input type="text" value="Candee's Test Users"/>
 Url:	
Link Type:	
<input checked="" type="radio"/> URL (A Link To An External Resource)	
<input type="radio"/> Page (A Page On Your Site)	

Figure 27: Options available inside the edit role rules screen

The following information and options are available inside this screen:

- **Role Name** – field displaying the name of the existing role
- **URL** – this is the page that the user will be directed to after they login, you might want users with a role of administrator to be sent to a different page then users who are assigned a different role in the system


- **Priority** – the priority is used to determine which page the user should be sent to. The higher priority will determine if a user should be distributed to one URL versus another
 - **For example** if a user has both the Administrator Role and the Module Training role some priority needs to be defined as to which page the user should be directed to. If you set the priority higher on the Administrator role option, the user will be navigated to that URL instead of the Module Training role. It is possible to have as many role/URL redirection rules setup as you would like, and set the priority for each one (**note:** priority only makes a difference when the user has more than one role).
- **Additional Message** – message displayed to the user after signing in (see Figure 28)
-  - option for editing a role rule (see section 8.2)
- **Adding a new Rule Role** - option for adding a new role rule (see section 8.1)



Figure 28: Message displayed to the user after signing in

8.1 Adding a new Rule Role

The purpose of the rule role option is to allow you to define login rules based on the role the user has been assigned to. In order to add a new rule, choose option “Security Role Rules” from the “Control Panel”.

The lower part of that page contains options for adding a new role.

☐ **Role:**

☐ **Url:**

Link Type:
☒ URL (A Link To An External Resource)
☐ Page (A Page On Your Site)

Location: (Enter The Address Of The Link)

[Select An Existing URL](#)

☐ **Priority:**

☐ **Additional Message (Optional):** ☐ Editor: ☐ Basic Text Box ☒ Rich Text Editor

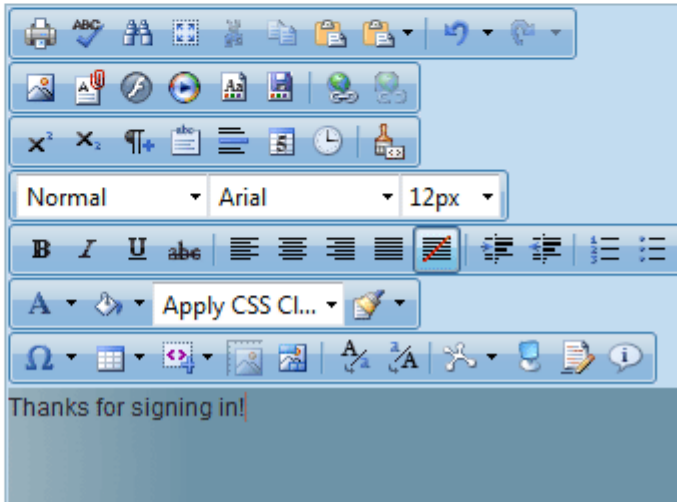


Figure 29: Adding a new Security Role

The following parameters are available inside this screen:

- **Role** – choose the desired role this rule will be applied to
- **URL** – set the rule for the URL user will visit after logging in
 - **URL (A Link To an External Resource)** – select this radio button if you want the user to visit external resource after logging in (**note:** the actual URL is entered inside the “Location” field)
 - **Page (A Page on Your Site)** – select this radio button if you want the user to visit a page on your website after logging in (**note:** the actual URL is entered inside the “Location” field)
 - **File (A File on Your Site)** – select this radio button if you want the user to download or visit a file on your site
 - **Location: (Enter the Address of the Link)** – input field for entering the URL (http://www.address.com)

- **Select an existing link** – option for selecting and managing existing links (see section 8.1.1)
- **Priority** – same as above for rules but it applies to users
- **Additional Message (optional)** – text area for entering any additional message you want to display to users who are assigned to specific role

After setting these parameters click on the “Update” button in order to save the changes and complete the procedure of adding a new rule.

8.1.1 Managing existing links

In order to select and manage existing URL, click on the “Select an Existing URL” link.

Role: Registered Users

Url:

Link Type:

☒ URL (A Link To An External Resource)

☐ Page (A Page On Your Site)

Location: (Enter The Address Of The Link)

http://www.registeredusers.com

Select An Existing URL

Figure 30: Choosing option "Select an Existing URL"

The following screen will be displayed.

Role: Administrators

Url:

Link Type:

☒ URL (A Link To An External Resource)

☐ Page (A Page On Your Site)

☐ File (A File On Your Site)

Location: (Enter The Address Of The Link)

http://dutch.datasprings.com

Delete Selected URL From The List


Add A New URL

Figure 31: Managing existing links

The following options are available inside this screen:

- **Location** – pull down menu containing existing links you can choose from
- **Delete Selected URL From the List** – use this option after choosing the desired link in order to delete it from the list
- **Add a New URL** –use this option in order to add a new URL to the list (pull down menu)


8.2 Editing an existing role rule

In order to edit an existing role click on this icon  next to the desired role name.


Control Panel

Data Springs Dynamic Login Control Panel


Visibility: ^




Manage Template




Module Configuration




Security Role Rules




Security Role Group Rules




User Notifications



Restrict by IP / SQL Validation






Single Sign On



Exit

Security Role Rules allow you to redirect the user or display unique messages to the user based on a specific security role. These security role rules are not valid for admin or host users and can be setup based on priority (higher priority number means a higher priority). Note: If you are setting up multiple security role rules, YOU MUST define unique priority levels such as 100, 200, 300, etc...

	Role Name	Url	Priority	
	admin		0	×
	Registered Users	http://www.registeredusers.com	4	×
	Subscribers	http://www.registeredusers.com	2	×

Role:

admin

Url:

Link Type:

☒ URL (A Link To An External Resource)
 ☐ Page (A Page On Your Site)

Figure 32: Editing an existing role

The screen with the parameters set for this rule will be displayed where you can change the desired information. Click on the “Update” button to save the changes.

Note: see section 8.1 for further information about the available parameters.

9 MANAGING SECURITY ROLE GROUP RULES

The "Security Role Group Rules" are very similar to Role rules. The Role Group is used for grouping i.e. organizing individual roles. In order to start setting up the groups, choose option "Security Role Group Rules" in the "Control Panel".



Figure 33: Choosing the "Security Role Group Rules" option

The following screen will be displayed.

	RoleGroupName	Url	Priority	Message
	West Coast		0	
	East Coast		0	
	Midwest		0	

Role Group:

Url:

Link Type:
☒ URL (A Link To An External Resource)
☐ Page (A Page On Your Site)

Location: (Enter The Address Of The Link)

[Select An Existing URL](#)

Priority:

Additional Message (Optional): ☐ Editor: ☐ Basic Text Box ☒ Rich Text Editor

Figure 34: Managing Role Group Rules

The following parameters and options are available inside this screen:

- option for editing the existing rule
- the option for deleting the rule
- The rest of the options are for adding the new group** – see section 9.1

9.1 Adding a New Role Group Rule

In order to start adding a new group rule, choose option “Security Role Group Rules” from the “Control Panel”. The following page will be displayed.

Role Group:

Uri:

Link Type:

☒ URL (A Link To An External Resource)

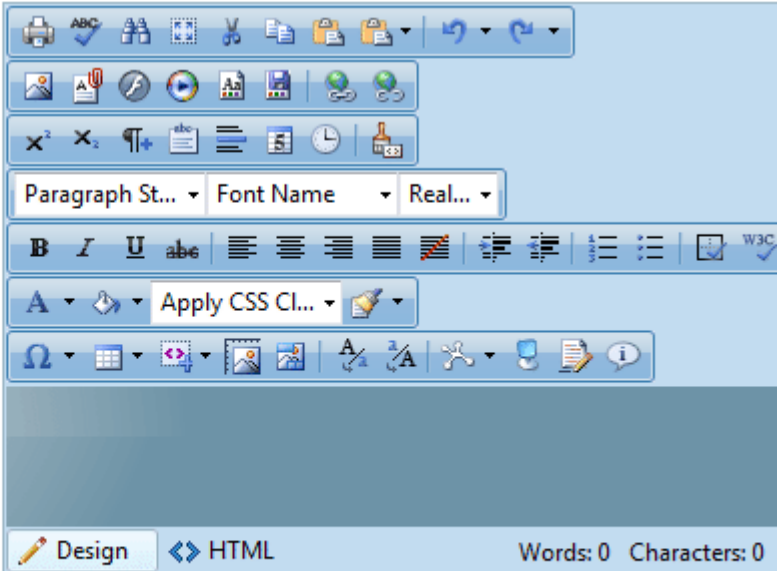
☐ Page (A Page On Your Site)

Location: (Enter The Address Of The Link)

Select An Existing URL

Priority:

Additional Message (Optional): ☒ Editor: ☐ Basic Text Box ☒ Rich Text Editor



Update

Figure 35: Adding a new group rule

The following options and parameters are available:

- **Role Group** – choose the desired role group from this pull down menu
 - **Note:** To add roles to role groups you should go to Admin, Security Roles, and clicking Edit within a security role. You will see that you can then set the role group. For example you might want to put the security role ‘California’ and the security role ‘Nevada’ into the security role group ‘West Coast’ but you might want to put the security role ‘Missouri’ and the security role ‘Kansas’ into the “Midwest Security Role Group’.
- **URL** – set the rule for the URL user will visit after logging in
 - **URL (A Link To an External Resource)** – select this radio button if you want the user to visit external resource after logging in (**note:** the actual URL is entered inside the “Location” field)
 - **Page (A Page on Your Site)** – select this radio button if you want the user to visit a page on your website after logging in (**note:** the actual URL is entered inside the “Location” field)

- **File (A File on Your Site)** – select this radio button if you want the user to download or visit a file on your site
- **Location: (Enter the Address of the Link)** – input field for entering the URL (http://www.address.com)
- **Select an existing link** – option for selecting and managing existing links (see section 8.1.1)
- **Priority** – same as above for rules but it applies to users
- **Additional Message (optional)** – text area for entering any additional message you want to display to users who are assigned to specific role

Edit Security Roles ▾

Basic Settings

In this section, you can set up the basic settings for this role.

Role Name:

Description:

Role Group: ▾

Public Role? ☐

Auto Assignment? ☐

Advanced Settings +

[Update](#) [Cancel](#)

Figure 36: Example of the role groups

10 MANAGING USER NOTIFICATIONS

The “Dynamic Login” module allows you to setup email notifications which will be sent to you in case the specified user(s) login. In order to start managing the user notifications, choose “User Notifications” from the control panel.



Figure 37: Managing the user notifications

The following page will be displayed.

	First Name	Last Name	Send Admin Notification
	Jon	Smith	<input checked="" type="checkbox"/>
User:	<input type="text"/>		
Additional Message:	Editor: <input type="radio"/> Basic Text Box <input checked="" type="radio"/> Rich Text Editor		
<div> </div>			
<div> <input checked="" type="radio"/> Send Admin Notification: <input type="checkbox"/> </div>			
<div> Update </div>			

Figure 38: Managing the user notifications


The following options and parameters are available:


- **Filter Criteria** – use this option to filter the user list based on the desired criteria (e.g. enter “John” to display all users with the first name “John”)



- **User** – enter the user name of the user you wish to add, e.g. johnsmith (**note:** you must provide a correct username in order for the notification to work properly)
- **Additional Message** – use this field to display a message to the user once they sign in.
- **Send Admin Notification** – select this checkbox to enable the admin notification feature
 - the e-mail template for this message can be setup within the module configuration section under “Admin Notification Email Template”(see section 13.4)

Once you add the desired user and optionally enter the additional message click “Update” and the user will be added i.e. you will start receiving notifications each time the specified user logs to the system.

Note: The additional message is the message the user will receive upon successfully signing into the system. The admin notification is a separate email that will notify the admin when a user has signed in.

	First Name	Last Name	Send Admin Notification
	Jon	Smith	<input checked="" type="checkbox"/>

 **User:**

 **Additional Message:**  **Editor:** ☐ Basic Text Box ☒ Rich Text Editor




Figure 39: User successfully added to the list

11 RESTRICTING BY IP/SQL VALIDATION

In order to start using the options for restricting users based on IP and SQL validation, choose the “Restrict by IP/SQL Validation” option from the control panel.



Figure 40: Restricting by IP/SQL validation

The following page will be displayed.

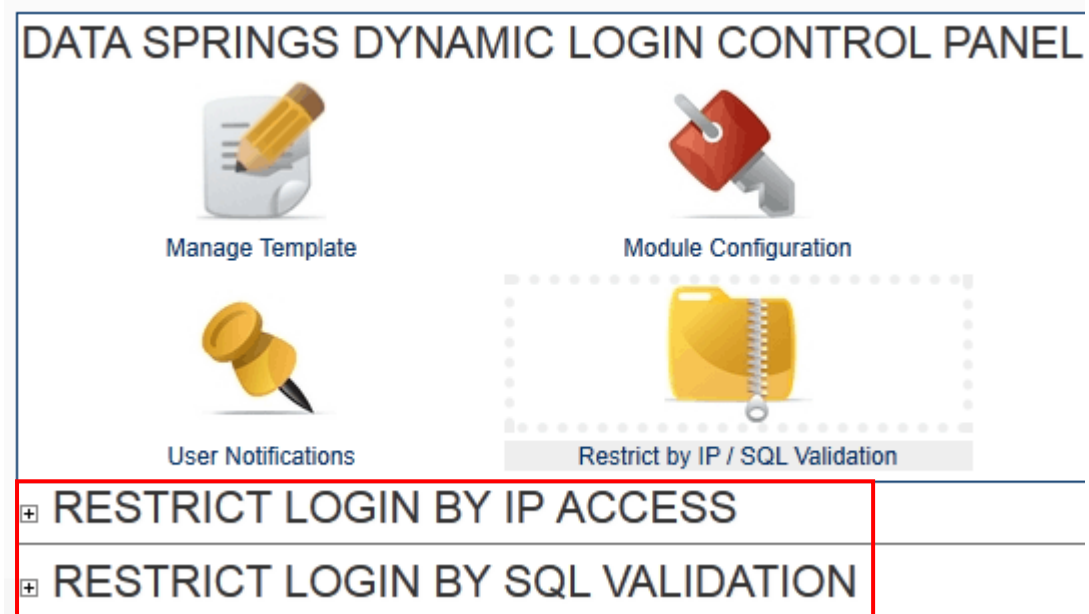


Figure 41: Restricting by IP and SQL validation

The following options and parameters are available:

- **Restrict Login by IP access** – see section 11.1
- **Restrict Login by SQL validation** – see section 11.2

11.1 Restricting Login by IP access

The “Dynamic Login” module allows you to restrict access to the portal by blocking specific IP addresses. In order to start using this option click + next to the “Restrict Login by IP Access” label.

☐ RESTRICT LOGIN BY IP ACCESS

Need to block out specific users from signing in based on their IP Address? You can block out specific that specific IP address for all instances of Dynamic Login within all portals of the DNN installation.

IP Address	Description	Affects All Module Instances?		
194.247.199.194		No		
194.247.199.195		No		
194.247.199.196		No		
		<input type="checkbox"/>		

Restricting Login by IP access

The following options and parameters are available:

- **IP Address** – displays the restricted IP addresses
- **Description** – displays the reason for the restriction
- **Affects All Module Instances** – displays information on whether this restriction should affect all module instances
- - the option for deleting the IP address from the list of blocked IP addresses, there fore allowing access to that IP address
- - the option for editing the desired entry
- - the option for blocking an IP address (see section 11.1.1)

11.1.1 Blocking an IP address

The IP addresses are blocked by adding them to the list of restricted addresses.

☐ RESTRICT LOGIN BY IP ACCESS

Need to block out specific users from signing in based on their IP Address? You can block out that specific IP address for all instances of Dynamic Login within all portals of the DNN installa

IP Address	Description	Affects All Module Instances?		
194.247.199.194		No		
194.247.199.195		No		
194.247.199.196		<input type="checkbox"/>		

Figure 42: Blocking an IP address

In order to block an IP address enter the desired IP address into the “IP Address” field and click this icon . The IP address will be blocked.

Note: you can choose to restrict the IP address from all module instances by clicking the checkbox.

11.2 Restricting Login by SQL validation

The “Dynamic Login” feature allows you to restrict login via SQL validation. You can block out specific users by enabling this feature and returning a query with one row/one column called IsValid.

If the column returns '0' or 'False' then the user will not be allowed to log in and will be presented with the error message. Any other value will be considered valid and will allow the user to sign in.

In order to start using this option, click + next to the “Restrict Login by SQL Validation” label.

RESTRICT LOGIN BY SQL VALIDATION

Need to block out specific users from signing in based on a SQL query? You can block out specific users by enabling this feature and returning a query with one row/one column called IsValid. If the column returns '0' or 'False' then the user will not be allowed to log in and will be presented with the error message. Any other value will allow the user to sign in.

Enable SQL Validation?: ☐

SQL Validation Query (should return one column called IsValid):

Validation Error Message:

Save

Exit Control Panel

Figure 43: Restricting Login by SQL validation

The following options and parameters are available:

- **Enable SQL Validation** - select the this checkbox to enable the SQL Validation for this module instance
- **SQL Valication Query (should return one column called IsValid)** - Enter the query for this validation. Parameters for the query can include the following tokens:
 - \$(UserID)
 - \$(PortalID)
 - \$(IPAddress)
- **Validation Error Message** - enter the validation error message which will be displayed to the restricted user

After setting the desired parameters, click “Save” to save the changes.

12 MANAGING SINGLE SIGN ON

The “Single Sign On (SSO)” functionality allows users to login with the same login credentials within other portals on the DNN® installation, as long as that users credentials exist in the parent portal. This will allow users to register on a single portal and have access to any other portals within the DNN® installation.

Additionally, once the user is authenticated within one portal their authentication will be automatically authenticated when they navigate between portals. This will allow you to enable you users to only login once and then continue browsing through a different portal as well without the need to login each time.

The functionality works as a system of master and slave portals and works in both directions. In other words, you can either replicate the user credentials from a master portal to a slave portal or the other way around, i.e. if the user logs into slave portal he will also be able to login to the master portal. The ability to use ‘Reverse SSO’ from the slave to master portals is an optional feature within the Single Sign On setup.

The system will also check the security roles for the user in 'Master Portal A' and add them to any matching security roles per name in 'Slave Portal B'.

For example: lets say that a user attempts to login on Portal B which already exists within Portal A with the security roles, 'Registered Users', 'Subscribers', and 'West Coast'. If these same security roles exist (by security role name) within Portal B they will automatically be added to these security roles within Portal B.

In order to start setting up the “Single Sign On” functionality, choose the “Single Sign on” from the control panel.



Figure 44: Managing Single Sign On

The following parameters and options are available:

- **Enable Single Sign On** – select this checkbox to enable the “Single Sign On”
- **Master portal** – select the master portal from this pull down menu. The master portal is the portal the system will attempt to authenticated the user against if they do not exist in the current portal.
 - If their authentication is valid within the master portal, the system will automatically add them as a valid user for the current portal
 - If their authentication is valid within the master portal the user will also be added to any security roles that they have to the new portal. The roles they are added to, are based on the ‘Role Name’. For example, if they have a role called ‘West Coast’ within the master portal (and the user is part of this role) and a role called ‘West Coast’ within the current portal. The user will be added to the ‘West Coast’ role within the child portal.
- **Add user to parent portal if user logs in and is not part of parent portal (Reverse SSO)** – select this checkbox if you wish to add the logged user to the parent portal if they do not exist within the parent portal and they login in successfully within the current portal.

- **Sync User Roles from Parent Portal for each Login?** - select this option if you would like the user security roles to always be synced with the master portal. If this feature is not enabled then the roles will only initially be added for the user on the child portal for the very first login. When this feature is enabled the roles will be synced from the master portal for each and every login.

After setting the desired parameters, click on the “Save” link to save the changes.

13 MANAGING MODULE CONFIGURATION

In order to start managing the module settings, choose option “Settings” from the main menu.



Figure 45: Choosing option "Module Configuration"

The following screen will be displayed.

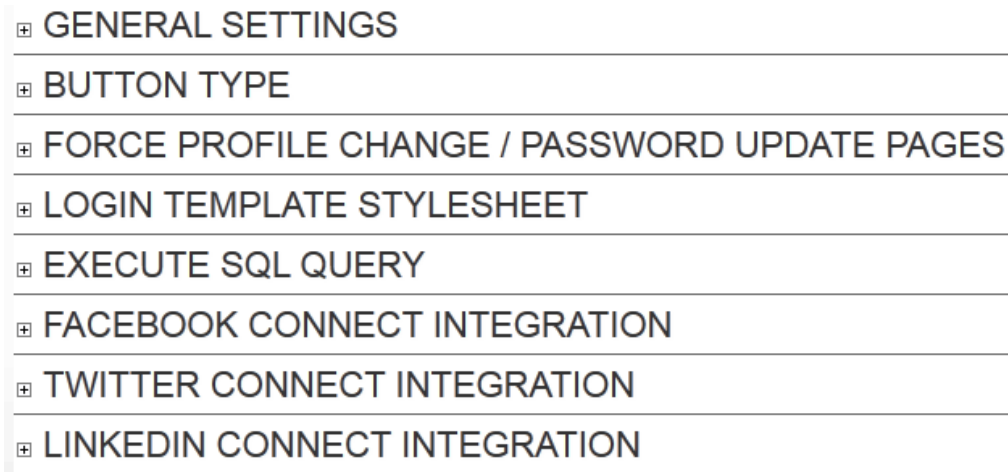


Figure 46: Choosing option "Dynamic Login Settings"

The following options are available:

- **General Settings** – see section 13.1
- **Button Type** – see section 13.2
- **Force Profile Change/Password Update Pages** – see section 13.3
- **Login Template Stylesheet** – see section 13.4
- **Execute SQL Query** – see section 13.5
- **Facebook Connect Integration** – see section 13.6
- **Twitter Connect Integration** – see section 13.7
- **Linked in Connect Integration** – see section 13.8

13.1 Managing the General Settings

In order to start managing the general module settings, click the plus sign next to the “General Settings” label.

GENERAL SETTINGS

Default Redirect Link: ☒ Link Type:

☒ URL (A Link To An External Resource)

☐ Page (A Page On Your Site)

Location: (Enter The Address Of The Link)

[Select An Existing URL](#)

Admin Notification Email Template: ☒

Override user and role redirection rules and always redirect to previous URL: ☒ ☐

Enable first time login message?: ☒ ☐

First time login message?: ☒

Allow user to login with their email address: ☒ ☐

Allow user to login with their User ID (separate from UserName): ☒ ☐

Keep user on same page as Dynamic Login module: ☒ ☐

Default Remember Me feature to true: ☒ ☐

Do not set focus to username field upon load?: ☒ ☐

Show background image for textbox fields: ☒ ☐

Username Watermark: ☒

Password Watermark: ☒

Hide Quick Menu (global setting): ☒ ☐

Figure 47: Managing the general settings

The following parameters are available inside the first part of the screen:

- **Default Redirect Link** – set the desired option for default redirect link
 - **URL (A Link To an External Resource)** – select this radio button if you want the user to visit external resource after logging in (**note**: the actual URL is entered inside the “Location” field)
 - **Page (A Page on Your Site)** – select this radio button if you want the user to visit a page on your website after logging in (**note**: the actual URL is entered inside the “Location” field)
 - **File (A File on Your Site)** – select this radio button if you want the user to download or visit a file on your site
 - **Location: (Enter the Address of the Link)** – input field for entering the URL (http://www.address.com)
 - **Select an existing link** – option for selecting and managing existing links (see section 8.1.1)
- **Admin Notification Email Template** – this is the template for the email message that you as an administrator will receive when a user signs in; this email message is sent when the checkbox “send notification” is selected (see section 6)
- **Override user and role redirection rules and always redirect to previous URL** – select this option if you wish to override any user or role redirection rules which apply to the users and always redirect them to the previous URL

- **Enable first time login message** - this setting will enable the message to the user the very first time they sign onto the system; this message will only be displayed in case the user has never signed on before
- **First time login message** – enter the text for the message the user will see the very first time they sign onto the system; you can use the tokens %Date%, %FirstName%, and %LastName% to customize the message per user
- **Allow user to login with their email address** – select this option if you wish to allow your users to use their email address as a username during the login
- **Allow user to login with their User ID (separate from UserName)** – select this option if you wish to allow your users to use their ID as a username during the login
 - **Note:** the UserID field is an integer (auto number) that is generated when a username is created.
 - **Example:** In some implementations you might want to simply send the user their UserID to login instead of having to remember their username. Often these implementations might be used in conjunction with another module such as Dynamic Registration to possibly allow the user to submit their information and receive a 'Ticket ID' or 'Claim ID' to login with which is actually their UserID.
- **Keep user on same page as Dynamic Login module** - this setting will keep the user on the same page as the Dynamic Login module; this page is useful when you want to include the login module on pages throughout your site forcing the user to click on the login link button
- **Default Remember Me feature to true** – select if you would like to enable the “Remember Me” checkbox to be defaulted to a value of true or initially checked when the user navigated to login page
- **Do not set focus to username field upon load** - If this setting is enabled the login form will not initially set the focus to the username textbox when the module loads
- **Show background image for textbox fields** - select this checkbox if you would like a background image to appear for fields such as username, password, and verification code; this setting will simply use an alternate CSS class when rendering these controls
- **Username Watermark** – enter the text which will be displayed within the username field before the user enters any values
- **Password Watermark** – enter the text which will be displayed within the password field before the user enters any values
- **Hide Quick Menu (Global Setting)** - select this option if you would like to hide the quick menu control panel for admin users on the user-facing page; this is a global setting which will hide the quick menu for all module instances within the entire web site

13.2 Setting the Button Type

In order to start setting the desired button type, click the plus sign next to the “Button Type” label. The following page will be displayed.

BUTTON TYPE

Input Button Type:

Link Buttons

Default Login Image Link:

Link Type:

☒ URL (A Link To An External Resource)

☐ File (A File On Your Site)

Location: (Enter The Address Of The Link)

http://

Select An Existing URL

Default Register Image Link:

Link Type:

☒ URL (A Link To An External Resource)

☐ File (A File On Your Site)

Location: (Enter The Address Of The Link)

http://

Select An Existing URL

Default Password Reminder Image Link:

Link Type:

☒ URL (A Link To An External Resource)

☐ File (A File On Your Site)

Location: (Enter The Address Of The Link)

http://

Select An Existing URL

Figure 48: Setting the button type

The following options and parameters are available:

- **Input Button Type** – choose the desired button type for this module instance; this can either be a link button, image button or standard HTML buttons
- **Default Login Image Link** – use this option to select the desired image you wish to use as a **login** link (see image below); you can either choose the file which has already been uploaded from the **File Name** pull down menu or use the **Upload New File** option to upload a new file from your PC
- **Default Register Image Link** - use this option to select the desired image you wish to use as a **Register** link (see image below); you can either choose the file which has already been uploaded from the **File Name** pull down menu or use the **Upload New File** option to upload a new file from your PC
- **Default Password Reminder Image Link** - use this option to select the desired image you wish to use as a **Reminder** link (see image below); you can either choose the file which has already been uploaded from the **File Name** pull down menu or use the **Upload New File** option to upload a new file from your PC

Page: 40 / 54

13.3 Forcing Profile Change/Password Update Pages

In order to start managing this setting, click the plus sign next to the “Force Profile Change/Password Update Pages” label. The following page will be displayed.

FORCE PROFILE CHANGE / PASSWORD UPDATE PAGES

Redirect page for invalid profile (required fields missing): ☒ Link Type:

☒ URL (A Link To An External Resource)

☐ Page (A Page On Your Site)

Location: (Enter The Address Of The Link)

http://

[Select An Existing URL](#)

Redirect page for password change (if Admin has selected to force the user to change their password.): ☒ Link Type:

☒ URL (A Link To An External Resource)

☐ Page (A Page On Your Site)

Location: (Enter The Address Of The Link)

http://

[Select An Existing URL](#)

Figure 49: Forcing Profile Change/Password Update Pages

The following options are available:

- **Redirect page for invalid profile (required fields missing)** – this setting will determine the page the user will be redirected to if their profile is not valid. In order to enable this setting you must also select to require a valid profile within the DNN Core System. You can complete this task under Admin, User Accounts, User Settings for the setting to require a valid profile for login. This page should redirect to a page such as Dynamic Registration that can allow the user to complete fields that are marked as required for their profile to be valid. Required fields for their profile are setup and defined under Admin, User Accounts, Manage Profile Properties.
- **Redirect page for password change (if Admin has selected to force the user to change their password)** - this setting will allow the user to login using their User ID. The UserID is a number assigned to each user created within the DNN portal and is separate from their UserName.

13.4 Managing the Login Template Stylesheet

In order to start managing the login template stylesheet, click the plus sign next to the “Login Template Stylesheet” label. The following page will be displayed.



Figure 50: Managing the Login Template Stylesheet

Use this text area to modify the stylesheet and click “Save Settings” to save the changes.

13.5 Executing an SQL Query

In order to start defining the custom SQL query, click the plus sign next to the “Execute SQL Query” label. The following page will be displayed.

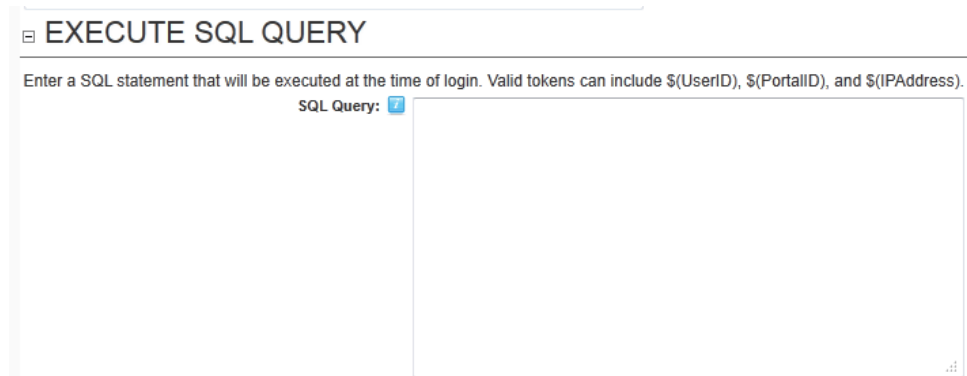


Figure 51: Executing an SQL Query

Use the “SQL Query” text area to specify the SQL query which should be executed at the time of login. The following tokens can be used:

- \$(UserID)
- \$(PortalID)
- \$(IPAddress)

13.6 Facebook Connect Integration

In order to setup the Facebook Connect Integration click **Module configuration** within the **Control panel** and then click + symbol under **Facebook Connect Integration**.

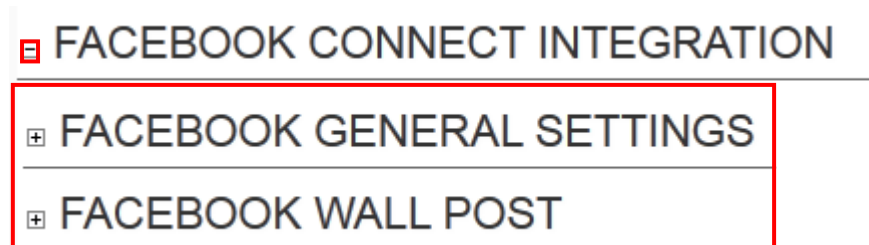


Figure 52: Available Facebook Connect options

The following options are available:

- **Facebook General Settings** – see section 13.6.1
- **Facebook Wall Post**– see section 13.6.1.1

13.6.1 Managing General Facebook Connect Settings

In order to start managing the general Facebook Connect settings, click the + symbol next to that label and the page will display all available options.

Facebook GENERAL SETTINGS

Facebook APP ID:

Facebook App Key:

Facebook APP Secret:

User Creation Type: ☐ None / Silent Post / Redirect to Thank You ☐ Facebook UserID
☐ Facebook EmailAddress

Redirect / Thank you page:

Username Prefix:

Authenticate user account with matching email address: ☐

Store UserID in Alternate Field: - Select DotNetNuke Field -

Store User Creation Status in Alternate Field: - Select DotNetNuke Field -

Extended Permissions:

OAuth 2.0 Page Type: PopUp Page

Alternate Image:

Submit HTTP Post: None

Silent Post (Dynamic Forms/ Registration URL):

Silent Post Details:

Figure 53: Managing General Facebook Connect Settings

The following options and parameters are available:

- **Facebook APP ID** - enter your Facebook APP ID, which can be retrieved from <http://developers.facebook.com>
- **Facebook App Key** - enter your Facebook APP Key which can be retrieved from <http://developers.facebook.com>
- **Facebook APP Secret** - enter your Facebook APP Secret. This APP Secret can be retrieved from <http://developers.facebook.com>
 - **Notes:**
 - Please reference this exact page for creating your application initially: <http://www.facebook.com/developers/apps.php>
 - You will need to click 'Set Up New App' to start.
 - During the wizard you should enter the domain name correctly and once you click **Save** you will receive your AppID, App Key and App Secret.
 - You can name the application whatever you want i.e. "Your-Company-name Authentication Tool" or similar; it does not have to be called "Dynamic Login Connect". This is setup and defined whenever you create the initial application at developers.facebook.com and you define your application name and will be present when it posts to the user is prompted for login, and the application posts to the users Facebook wall.
- **User Creation Type** – choose the method for creating Facebook authenticated users. Users can either be created based on their Facebook UserID or with their email address as their username.
- **Redirect / Thank you page** - enter the URL the user will be taken too if you choose 'None' as the user registration method.
 - **Note:** the user will only be taken to this page if "None" is selected and if the users credentials don't match a valid login. In this case you might consider using a

feature such as the Silent Post to post details to Dynamic Registration to create the user instead of creating the user through this integration

- **Username Prefix** - enter a prefix in case you wish to add it to each user created via Facebook Connect or OAuth integration (**note:** this can help you differentiate these users from all other users in the system).
- **Authenticate user account with matching email address** - select this option if you would like to authenticate and match user's Facebook account with his DotNetNuke User Account based on their email address
- **Store UserID in Alternate Field** - select a DotNetNuke profile field for storing the Facebook UserID
 - **Note:** this can be useful if you are creating the username based on the email address but would still like to have access to the Facebook UserID field for the future
- **Store User Creation Status in Alternate Field** - select a DotNetNuke profile field which for storing information on how the user was created (i.e. Facebook Connect, or Facebook OAuth). This feature can help you identify users created via the Facebook Integration
 - **Note:** when implemented this feature will store a value of "FacebookUser" to the profile field (in future versions this will also be a feature that can be used for other authentication systems such as "Twitter" etc)
- **Extended Permissions** - Initially the parameters requested are for basic information including the users email address. You can optionally request additional information by passing in additional parameters in a comma separated list without spaces. The list of extended permissions is located at <http://developers.facebook.com/docs/authentication/permissions/>
- **Example:** user_about_me,user_birthday,user_likes.
 - **Note:** This can be useful if you are using this same application ID within other modules that might showcase these extended permissions.
- **OAuth 2.0 Page Type** - select the page type for the OAuth 2.0 authentication integration. This can include either a redirect page or a pop up page
- **Alternate Image** - please enter the name of an alternate image for the Facebook connection button.
 - **Important note:** this image must be located in the `/desktopmodules/dynamiclogin/images` directory
 - Several alternate images are already included within the Dynamic Login installation – these include facebook1.gif, facebook2.gif, facebook3.gif, facebook4.gif. You can demo what these look like here:
 - [Default Image](#)
 - [Facebook1.gif](#)
 - [Facebook2.gif](#)
 - [Facebook3.gif](#)
 - [Facebook4.gif](#)
 - Add your own! Just copy a file into the /images folder as noted above and reference it within this property.
- **Submit HTTP Post** - select the desired option for submitting an HTTP post among the following:
 - **Creating User Only** – choose this option to submit an HTTP post only in the case the user has been created
 - **Signing in User Only** – choose this option to submit an HTTP post only in the case the user has signed in

- **Creating User and Signing in User** – choose to submit an HTTP post in case the user has been created and has signed in
 - **Note:** An HTTP Post can be sent to any page/module but there are direct integration options with Dynamic Forms and Dynamic Registration
- **Silent Post (Dynamic Forms/ Registration URL)** - select the URL that you would like to post the Facebook account details to. This allows for the integration with Data Springs Dynamic Registration or Dynamic Forms module which can accept a silent post and process the registration and/or completion events there
- **Silent Post Details** - select the URL that you would like to post the Facebook account details to. This allows for the integration with Data Springs Dynamic Registration module which can accept registration data via a silent post and process the registration there
- **Note:**
 - Please check our site for recent blog posts and forum posts related to examples of silent posts. Soon we will be posting blogs on how to use the silent post with Dynamic Registration, Opt In Email, Dynamic Forms etc
<http://www.datasprings.com/news/blog>
 - You can also read our blog post [Receive Dynamic Forms / Dynamic Registration Silent HTTP Posts](#)

13.6.1.1 Managing Facebook Wall Post Settings

In order to start managing the Facebook Wall Post settings, click the + symbol next to that label and the page will display all available options.

FACEBOOK WALL POST

Post message to users wall?: ☐

Wall Post days delay check (0 for always):

Wall Post Title:

Wall Post Message:

Wall Post Link:

Wall Post Image:

Figure 54: Managing Facebook Wall Post Settings

The following options and parameters are available:

- **Post message to user's wall?** – select to enable posting to user's wall
- **Wall Post days delay check (0 for always)** - enter the desired time out during which the module should ignore the fact that the user signed in i.e. not post information on their wall
 - **For example**
 - If you put **30**, the module will post to the wall the first time and then wait for 30 days before posting the information again
 - If you enter **0** the module will post to the wall each time the user is logged
- **Wall Post Title** - enter the title for the wall post; this will be the title of the Facebook wall post when a user signs in through Facebook Integration
- **Wall Post Message** - enter the message for the wall post; this will be the message of the Facebook wall post when a user signs in through the Facebook Integration
- **Wall Post Link** – enter the URL or link for the wall post; this link should be the full path starting with http://. The link would normally be the web site that the user is signing in from
- **Wall Post Image** - select if you would like to post an image to the user's wall; this image will render to their Facebook wall each time they sign into your web site.

13.6.1.2 Facebook Connect from your Users' Perspective

This section will describe and illustrate using of Facebook Connect as seen by your users. The first step for your users is clicking the **Connect** button/image.

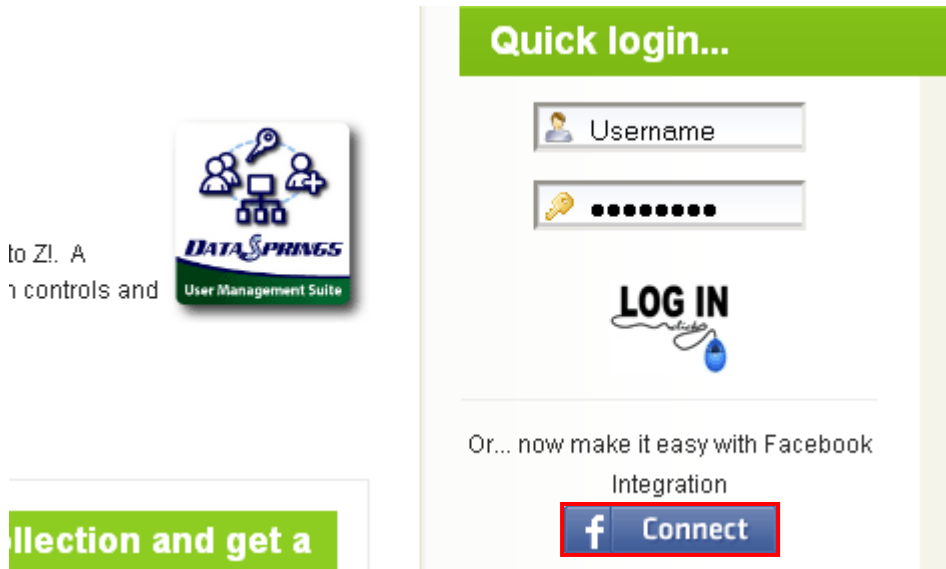


Figure 55: Facebook Connect as Seen by Your Users (1/4)

- **Note:** you can specify an alternate image for the connect button by using the **Alternate Image** parameter

Once you users click **Connect**, the permission request window will be displayed.

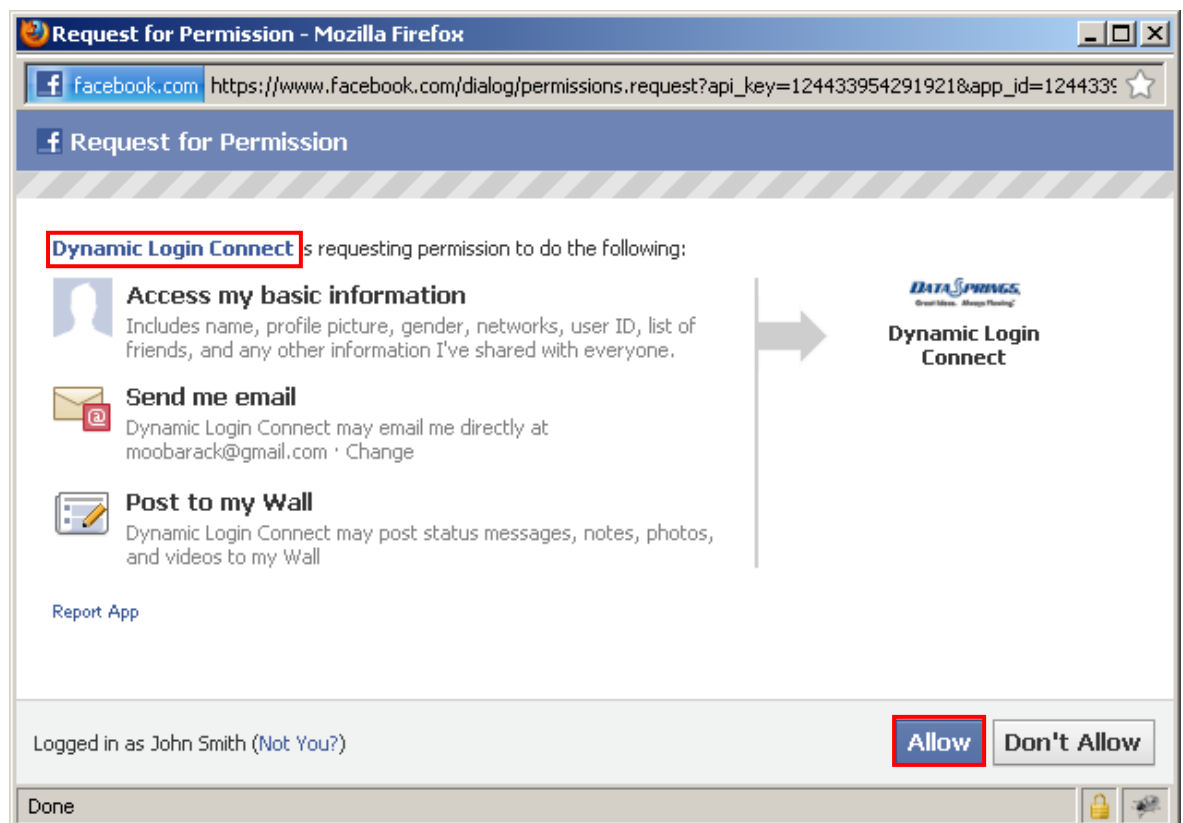


Figure 56: Facebook Connect as Seen by Your Users (2/4)

The upper left corner displays the name of the module i.e. **Dynamic Login Connect** (note: you can set a custom name). After your users click **Allow**, they will automatically be logged in into your site.

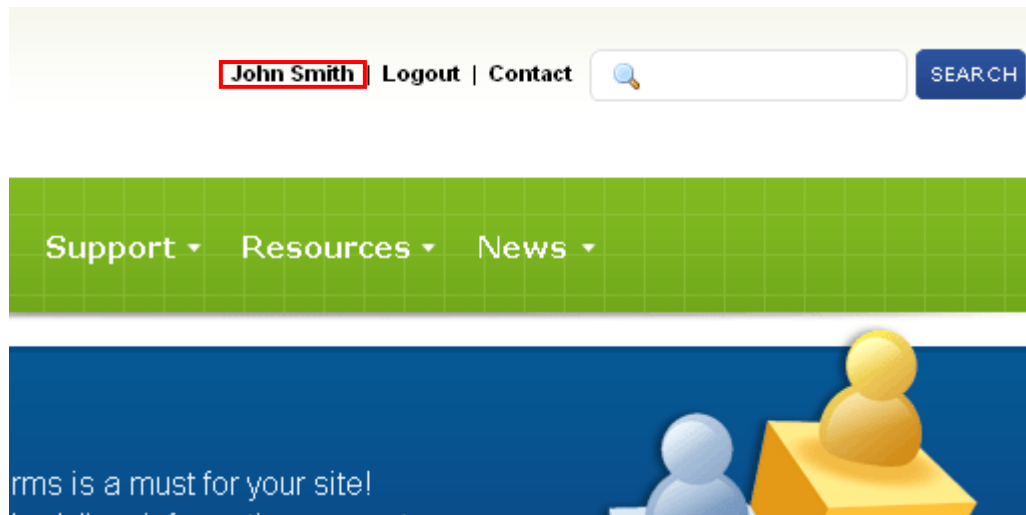


Figure 57: Facebook Connect as Seen by Your Users (3/4)

Also, in case you have enabled this feature, information about this will be posted to their wall (see 13.6.1.1).



Figure 58: Facebook Connect as Seen by Your Users (4/4)

Below is the screenshot which illustrates how the whole post has been setup in the backend.

FACEBOOK WALL POST

Post message to users wall?: ☒

Wall Post days delay check (0 for always):

Wall Post Title:

Wall Post Message:

Wall Post Link:

Wall Post Image:

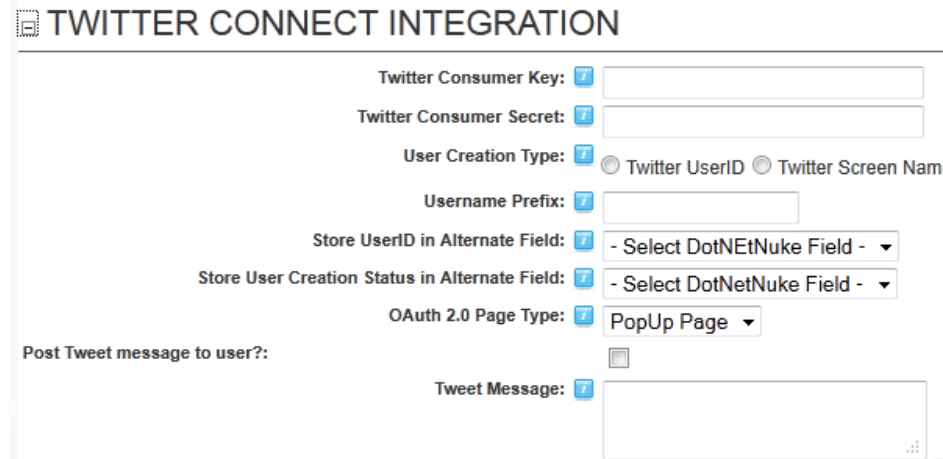
Figure 59: The way the wall post has been setup

Notes:

- The "I just signed into..." text is specified using the **Wall Post Message** parameter
- The bottom of the post shows the name of the module used for posting the information which is **Dynamic Login Connect**.

13.7 Setting up the Twitter Connect Integration

In order to setup the Twitter Connect Integration click **Module configuration** within the **Control panel** and then click + symbol under **Twitter Connect Integration**.



TWITTER CONNECT INTEGRATION

Twitter Consumer Key:

Twitter Consumer Secret:

User Creation Type: ☒ Twitter UserID ☐ Twitter Screen Name

Username Prefix:

Store UserID in Alternate Field: - Select DotNetNuke Field -

Store User Creation Status in Alternate Field: - Select DotNetNuke Field -

OAuth 2.0 Page Type: PopUp Page

Post Tweet message to user?: ☐

Tweet Message:

Figure 60: Setting up the Twitter Connect Integration

The following parameters are available:

- **Twitter Consumer Key** - please enter your TwitterConsumer Key. This Consumer Key can be retrieved from <https://dev.twitter.com>.
- **Twitter Consumer Secret** - please enter your TwitterConsumer Secret. This Consumer Secret can be retrieved from <https://dev.twitter.com>. Please review the documentation on www.datasprings.com for more information.
- **User Creation Type** - select how you would like Twitter authenticated users created. Users can either be created based on their Twitter UserID or they can be created with their screen name as their username.
- **User Prefix** - enter a prefix if you want the username to include a prefix for each user created via Twitter Connect or OAuth integration.
- **Store UserID in Alternate Field** - select a DotNetNuke profile field that you would like the Twitter UserID stored in. This can be useful if you are creating the username based on the email address but would still like to have access to the Twitter UserID field for the future.
- **Store User Creation Status in Alternate Field** - select a DotNetNuke profile field that you would like to store how the user was created (i.e Twitter Connect, or Twitter OAuth). This feature can help you identify users created via the Twitter Integration.
- **OAuth 2.0 Page Type** - select the page type for the OAuth 2.0 authentication integration. This can include either a redirect page or a pop up page.
- **Post Tweet message to user** – select if you wish to post a tweet to the user (enter the message in the field below)
- **Tweet Message** – please enter the message for the tweet post. This will be the message of the Twitter tweet post when a user signs in through the Twitter Integration.

13.8 Setting up the Linked in Connect Integration

In order to setup the Twitter Connect Integration click **Module configuration** within the **Control panel** and then click + symbol under **Linked in Connect Integration**.

LINKEDIN CONNECT INTEGRATION

LinkedIn API Key:
 LinkedIn Secret Key:
 Username Prefix:
 Store UserID in Alternate Field:
 Store User Creation Status in Alternate Field:
 OAuth 2.0 Page Type:
 Post Status message to user?: ☐
 Post Message:
 Save Settings

Figure 61: Setting up the Linked in Connect Integration

The following parameters are available:

- **LinkedIn API Key** - please enter your LinkedIn API Key. This API Key can be retrieved from <http://developer.linkedin.com/>. Please review the documentation on www.datasprings.com for more information.
- **Linked Secret Key** - please enter your LinkedIn Secret Key. This Secret Key can be retrieved from <http://developer.linkedin.com/>. Please review the documentation on www.datasprings.com for more information.
- **Username Prefix** - enter a prefix if you want the username to include a prefix for each user created via LinkedIn Connect or OAuth integration.
- **Store UserID in Alternate Field** - select a DotNetNuke profile field that you would like the LinkedIn UserID stored in. This can be useful if you are creating the username based on the email address but would still like to have access to the LinkedIn UserID field for the future.
- **Store User Creation Status in Alternate Field** - select a DotNetNuke profile field that you would like to store how the user was created (i.e LinkedIn Connect, or LinkedIn OAuth). This feature can help you identify users created via the LinkedIn Integration.
- **OAuth 2.0 Page Type** - select the page type for the OAuth 2.0 authentication integration. This can include either a redirect page or a pop up page.
- **Post Status message to user** – select if you wish to enable posting of the status message to the user
- **Post Message** - please enter the message for the user status post. This will be the message of the LinkedIn user status post when a user signs in through the LinkedIn Integration.

14 AUTO SIGN-IN FEATURE

The Auth Sign In feature is a new feature which listens for URL querystring parameters or a form post/http form post which will pass the user's information and direct them to a page of your choice by also signing them in without their knowledge.

14.1 Instructions for setting up Auto Sign in

Please follow these steps to setup the auto sign-in:

- Pass the login page the querystring parameter "autosignin" with a value of "True"
- Optionally pass the login page the querystring parameter of signintype. This value should be "Form" or "Querystring" and if left blank then the module will default to "Querystring".
- Depending in of the sign in type if "Form" or "Querystring" the users credentials should be passed via the form or querystring variables as "username" and "password"
- This feature allows you to setup other modules that might be able to pass along the sign in credentials to allow the user to be signed into the portal, and/or also something as simple as creating sign in link for users where they can click on the link directly and sign into the portal.

15 DROPDOWN LOGIN INTEGRATION SKIN OBJECT

This simple jQuery skin object allows the ability for the user to sign in without being forced to another login page, while also refreshing the current page the user is on after they are authenticated.

This skin object can be included in any skin and is completely controlled via CSS. Check out some different and unique styles that you could setup to easily control the look of DropDown Login.

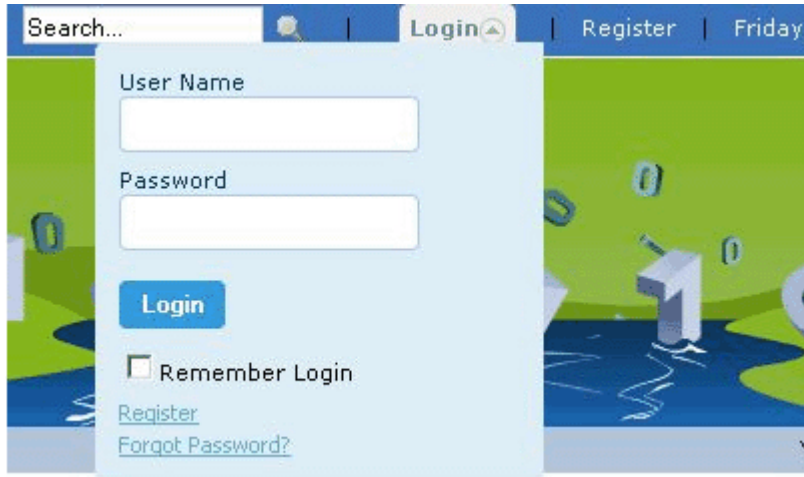


Figure 62: Example 1

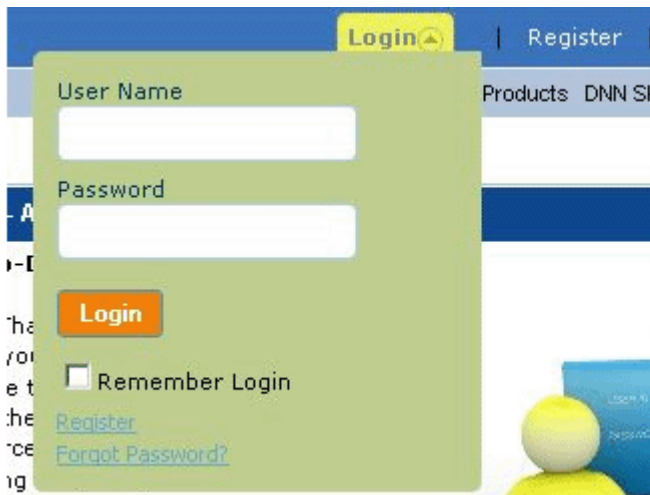


Figure 63: Example 2

15.1 Instructions on implementing this feature

Detailed instructions for implementing this feature can be found here on pages 3 and 4 of the [Drop Down Login User Guide](#) (PDF).

16 DELETING DYNAMIC LOGIN MODULE

In order to delete “Dynamic Login” module instance, choose option **Delete** from the main menu.

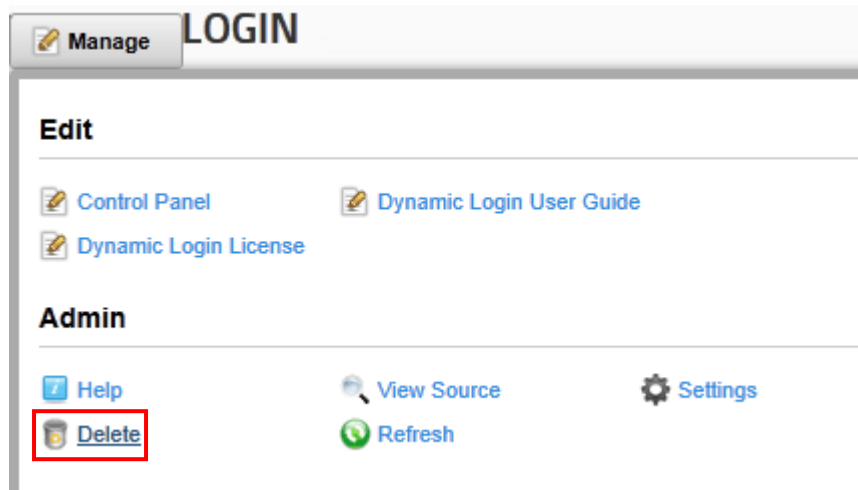


Figure 64: Deleting Dynamic Login (step 1/2)

The following screen will be displayed.

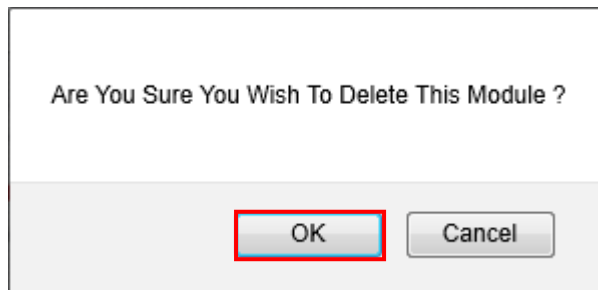


Figure 65: Deleting Dynamic Login (step 2/2)

Click on the **OK** button and the module will be deleted.