AD-Pro Authentication

'AD-Pro Authentication' is the most powerful Active Directory authentication provider for DNN Platform©. Leverage the power of Windows® Active Directory® by integrating DNN®, to seamlessly allow your users to login to DNN Platform with their AD credentials. Ideal for corporate intranets, Internet sites, secure extranets, schools, colleges and universities.

You can download the 'AD-Pro Authentication' 14 day free trial from: ⇗ http://store.dnnsoftware.com/home/product-details/active-directory-authentication-v35

1. Installation

Note: Objective of this chapter is to show how to install 'AD-Pro Authentication' module in your DNN website.

1.1. Requirements

- DNN Platform v8+
- .NET Framework 4.0+
- ASP.NET Full Trust levels
- ⇗ Connection Manager a DNN module from Glanton

1.2. Before you start

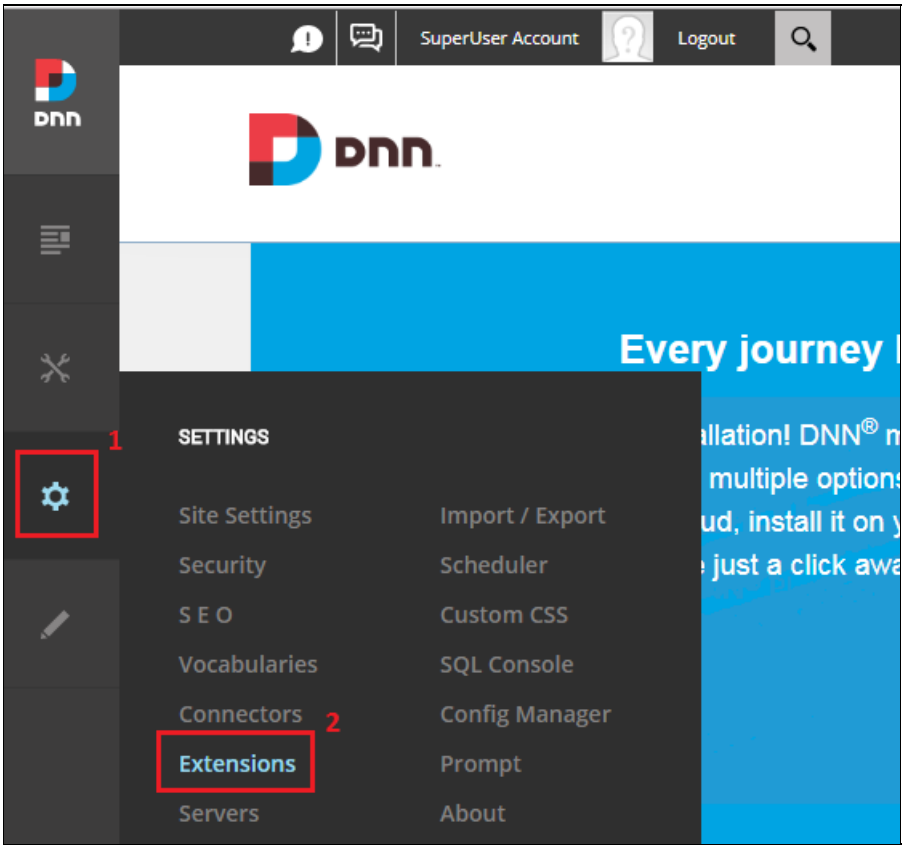
1. Make all backups, including DNN database and file system.
2. If "AD-Pro Authentication v2" (previous version of this module) exist - remove it. Previous version isn't compatible witch v3, and it can't be upgraded.
3. If ⇗ "DotNetNuke® Auth: Active Directory" exist in DNN Platform, disable that extension, then comment or remove following code snippet from the `web.config` file:

```
<location path="DesktopModules/AuthenticationServices/ActiveDirectory/WindowsSignin.aspx">
    <!-- Disable Forms Authentication -->
    <formsAuthenticationWrapper enabled="false" />
    <system.webServer>
        <security>
        <!-- Enable IIS Windows authentication for the login page -->
            <authentication>
                <windowsAuthentication enabled="true" useKernelMode="false">
                    <providers>
                        <clear/>
                        <add value="NTLM"/>
                    </providers>
                </windowsAuthentication>
                <anonymousAuthentication enabled="false" />
            </authentication>
        </security>
    </system.webServer>
</location>
```

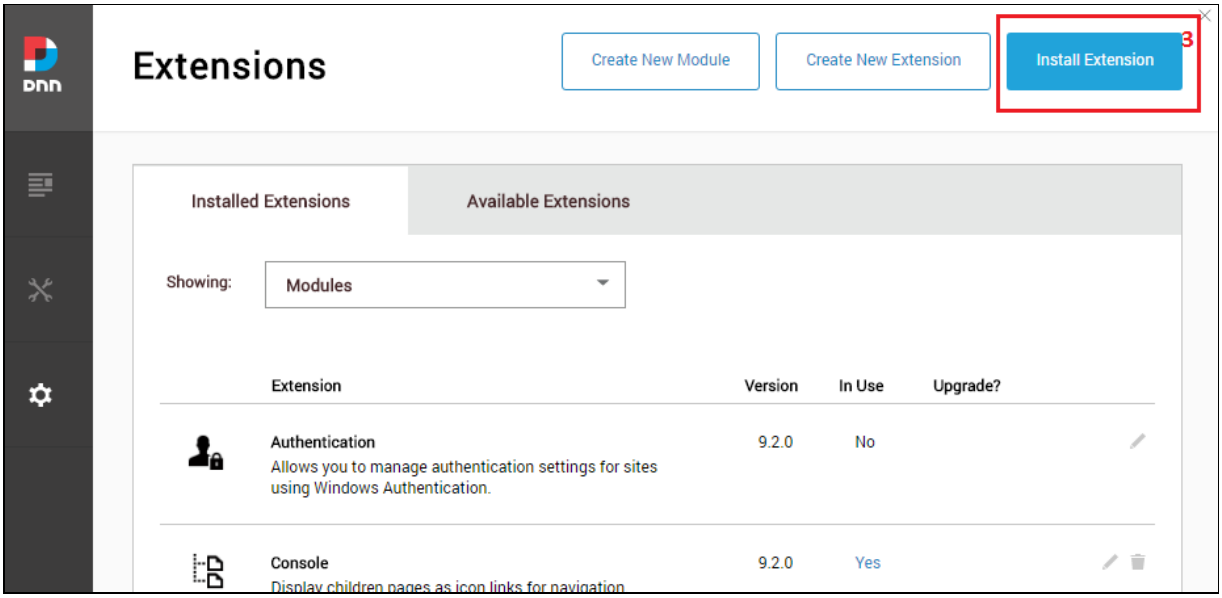
1.3. Module installation process

1. Sign in to the DNN website as a 'DNN Host'.

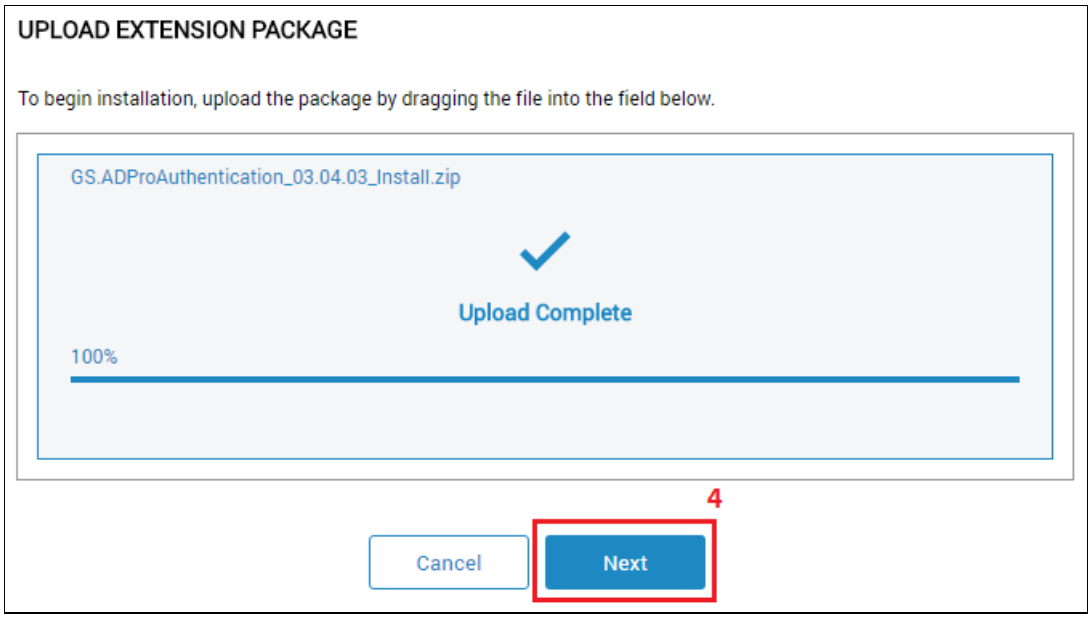
2. Go to 'Settings-> Extensions', see figure below.



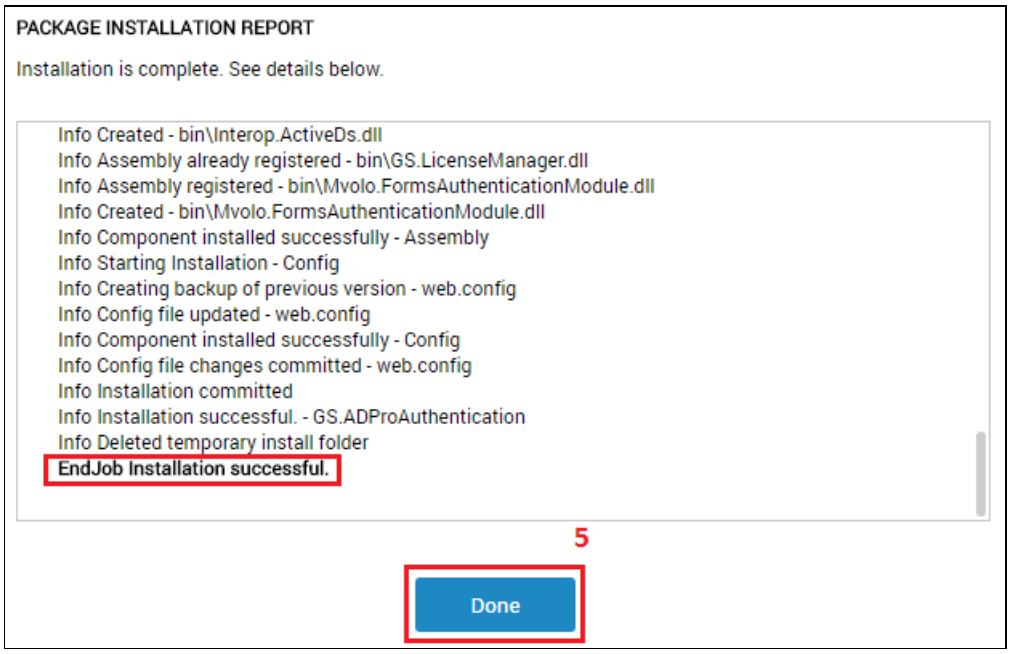
3. Click 'Install Extension' button, see figure below.



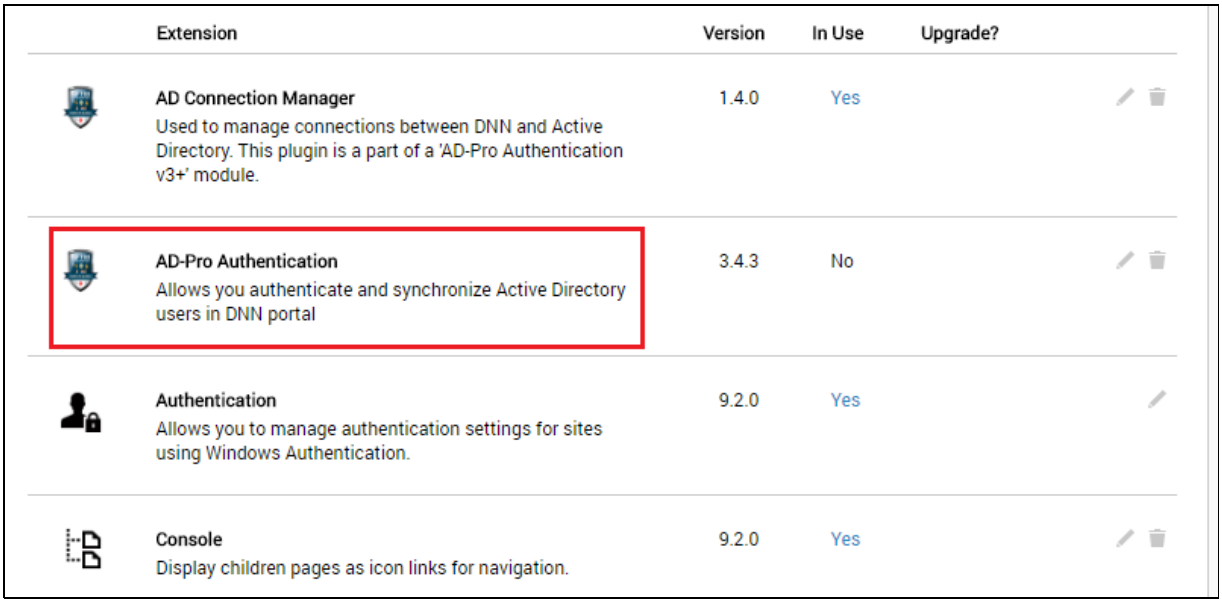
4. Upload extension package (see figure below) and click 'Next' button few times. This will take you through all steps of module installation wizard.



5. If package was successfully installed, following screen should appear. Click 'Done' button to finish this process.



6. Now extension list contain newly added module, the module version can be vary, see figure below.



1.4. Changes made during the module installation process

At the module installation process, following modifications will be automatically done:

1. In DNN database will be created table `GS_ADProAuth_Settings`

2. In DNN file system, under the `DesktopModules`, will be added folder `GS_ADProAuthentication`.

3. In `web.config` file, under node `<system.webServer><modules>`:

```
<remove name="FormsAuthentication" />
<add name="FormsAuthentication" type="Mvolo.Modules.FormsAuthModule" />
<add name="AdProAuthenticationModule"  type="GS.ADProAuthentication. AdProAuthenticationModule, GS.ADProAuthentication
```

4. In `web.config` file, at the end of the configuration section following node will be added:

```
<location path="DesktopModules/GS_ADProAuthentication/WinAuthSignIn.aspx">
    <!-- Disable Forms Authentication -->
    <formsAuthenticationWrapper enabled="false" />
    <system.webServer>
    <security>
        <!-- Enable IIS Windows authentication for the login page -->
        <authentication>
        <windowsAuthentication enabled="true" useKernelMode="false">
            <providers>
            <clear />
            <add value="NTLM" />
            </providers>
        </windowsAuthentication>
        <anonymousAuthentication enabled="false" />
        </authentication>
    </security>
    </system.webServer>
</location>
```

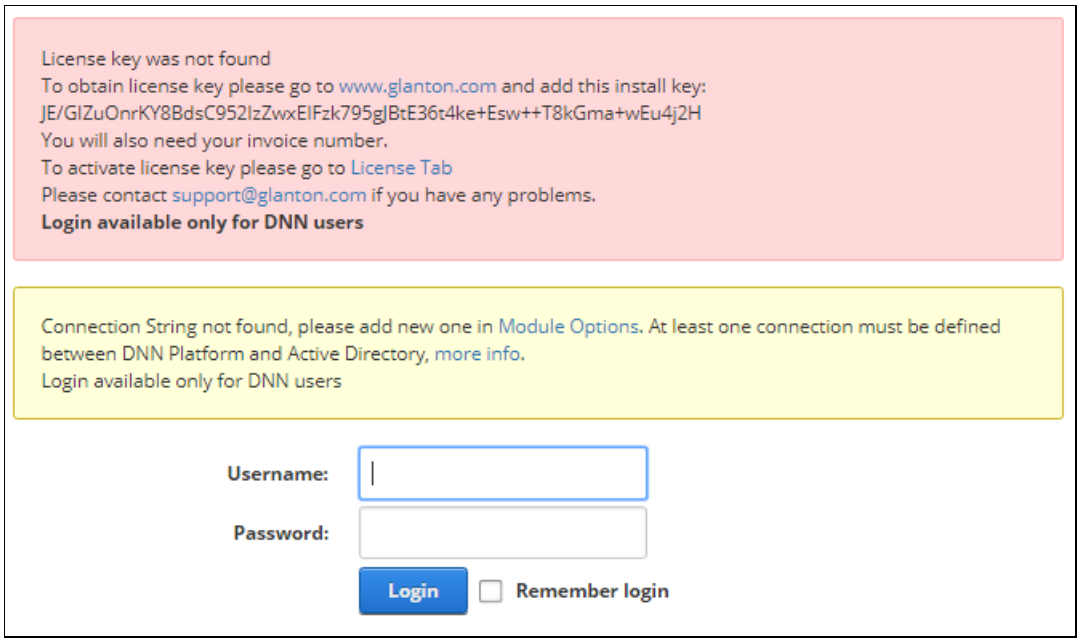
2. Product Activation

Note

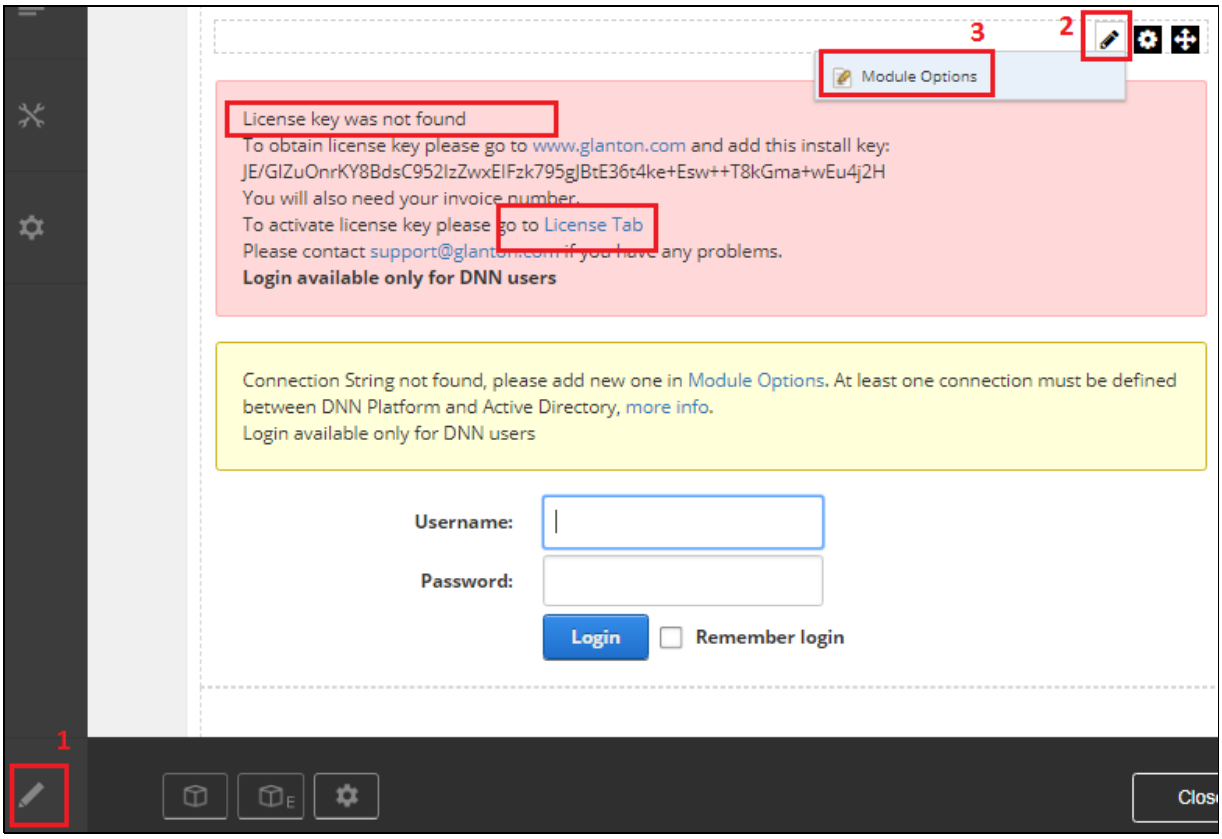
Objective of this chapter is to show how to apply license and activate “AD-Pro Authentication” plugin.
Before you read this chapter please get familiar with ⇗Licensing policy, where general licensing rules are described.
Product activation consist of three steps: obtain “Install Key”, generate “License Key”, and final activation.

1. Sign in to the DNN website as a “DNN Host” or “DNN Administrator”.

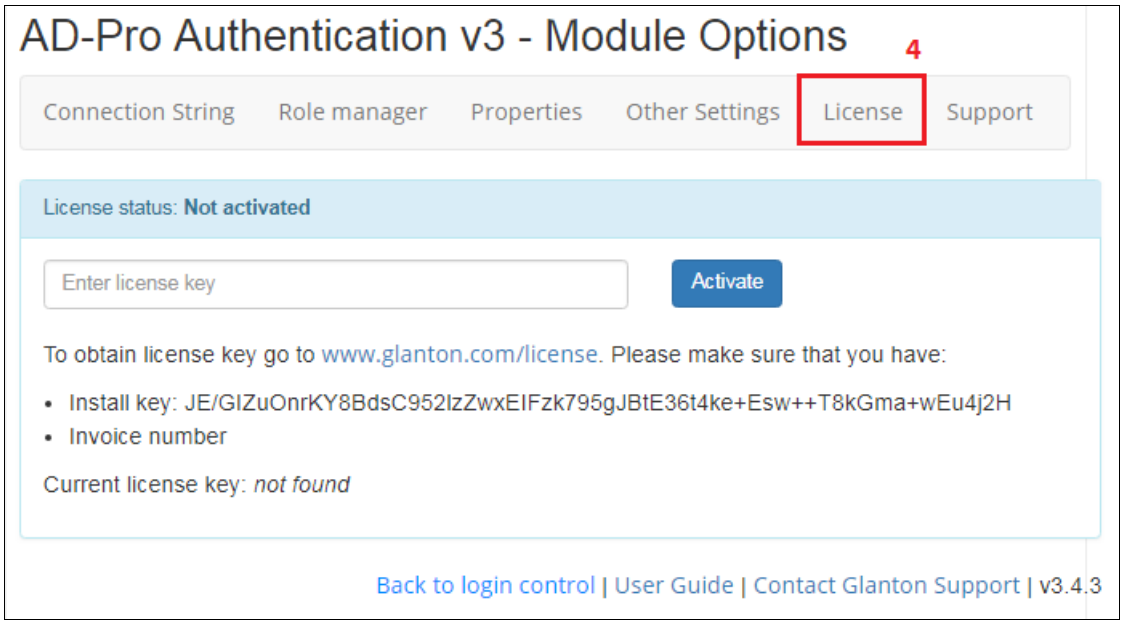
2. Go to page where ‘AD-Pro Authentication’ module is placed. If plugin is not activated, you should see message like on figure below.



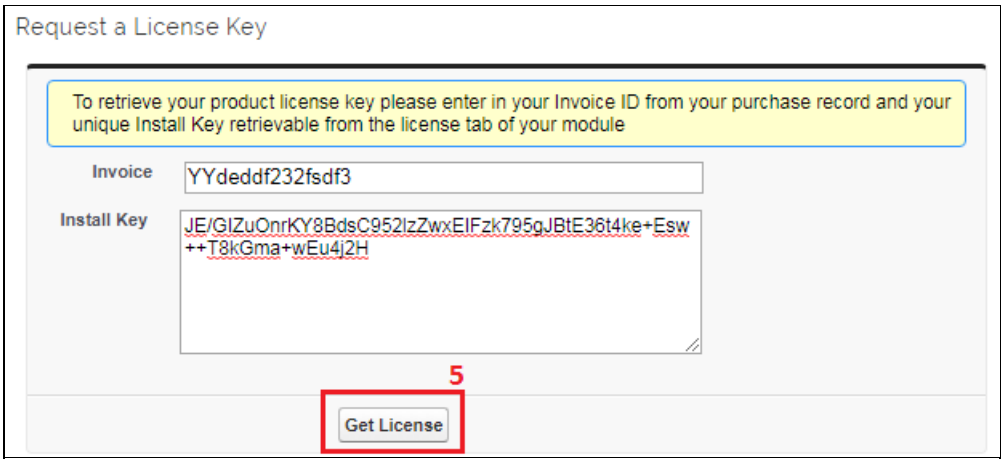
3. Set DNN into 'Edit' mode, then go to the 'Module Options', see figure below:



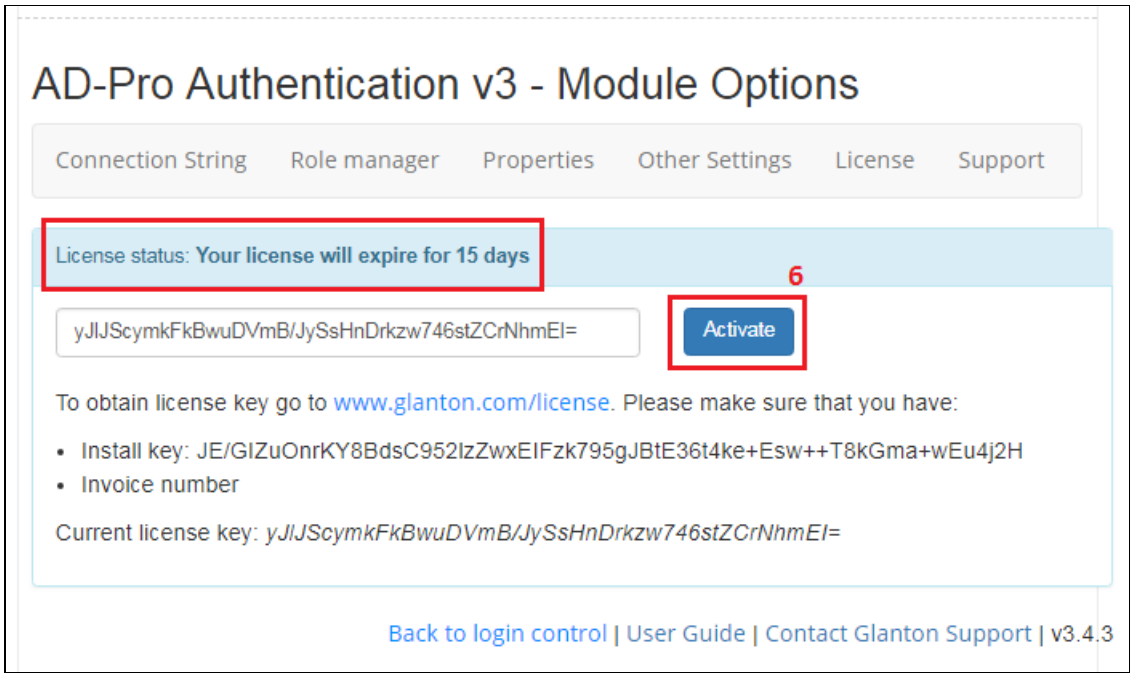
4. Go to 'License tab', see figure below.



5. Copy 'Install Key' and open License form, you should be redirected to page where is located form like on figure below. Paste 'Install Key', 'Invoice number' and click on 'Get License' button. This will genarate new 'License Key' for your product, copy license string.



6. Back to the 'License tab', apply 'License key' and activate product. If license key is correct you should get message like on figure below.



At the end of this process the 'AD-Pro Authentication' plugin should be activated.

3. Base Configuration

Note: Objective of this chapter is to show how set up initial envoironment for 'AD-Pro Authantication' plugin.

3.1. Overview

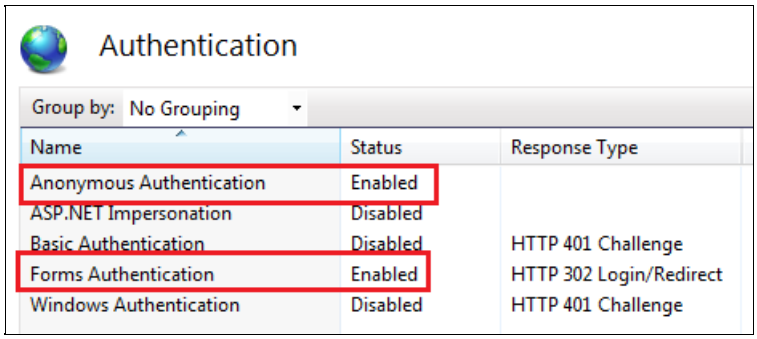
For the "AD-Pro Authentication" extension, following components needs to be changed:

- Internet Information Services (authentication section),
- DNN Platform (adjust the folder permissions),
- DNN Platform (section "Admin->Site settings"),
- and at the end some setings inside "AD-Pro Authentication" module,

3.2. Initial IIS configuration

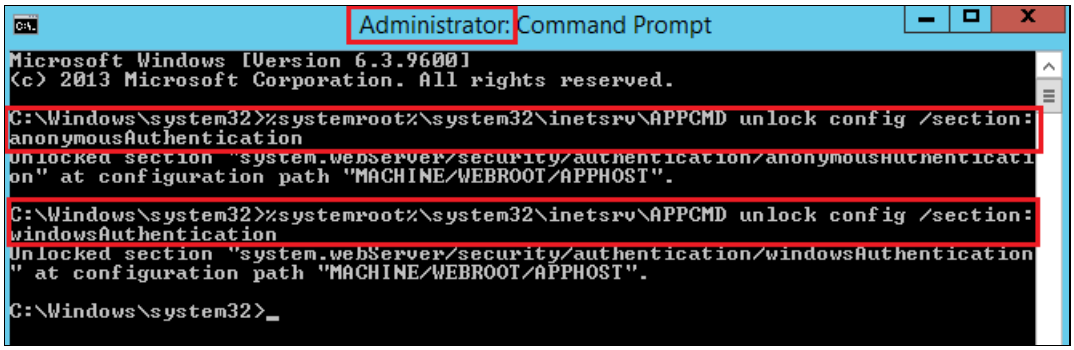
Before you install module:

1. Please make sure that in Internet Information Services (IIS) under 'Authentication' tab DNN Platform has settings as follows:



2. On the server where is the IIS, open 'Command line' (CMD) as 'Run As Administrator' and execute following commands. This will allow 'AD-Pro Authentication' plugin to automatically change 'IIS-> Authentication' settings for file: `DesktopModules/GS_ADProAuthentication/WinAuthSignIn.aspx`:

```
%systemroot%\system32\inetsrv\APPCMD unlock config /section:anonymousAuthentication
%systemroot%\system32\inetsrv\APPCMD unlock config /section:windowsAuthentication
```



Note

To start cmd.exe with Administrative privileges:

1. Open the Start menu.
2. Press the windows icon key.

- Click on the Start windows icon icon at the left end of the taskbar.
- Type cmd.exe in the search box.

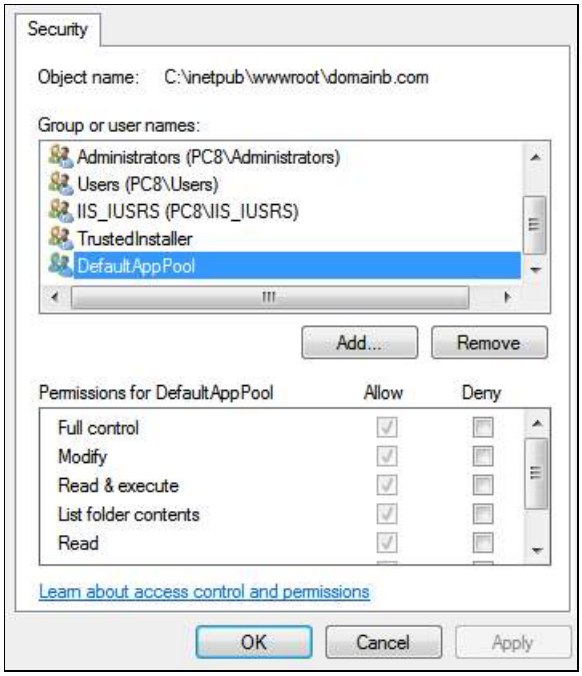
3. Press Ctrl + Shift + Enter.

This starts the Command Prompt as the Administrator user.

If these commands returns error like: `Object ' UNLOCK CONFIG /SECTION:ANONYMOUSAUTHENTICATION' is not supported` the changes in the `applicationHost.config` file located in the `%windir%\system32\inetsrv\config\` folder needs to be done. More info: ⇗http://www.iis.net/learn/get-started/planning-for-security/how-to-use-locking-in-iis-configuration

3.3. Initial file permissions

Make sure that file system permissions for directory where main DNN website is placed are correct. The `Application Pool Identity user` should have permissions: `read`, `write`, `modify`. Figure below describes correct permissions for DNN website located in folder: `c:\inetpub\wwwroot\domainb.com`, in this case `Application Pool Identity user` is called `DefaultAppPool`.

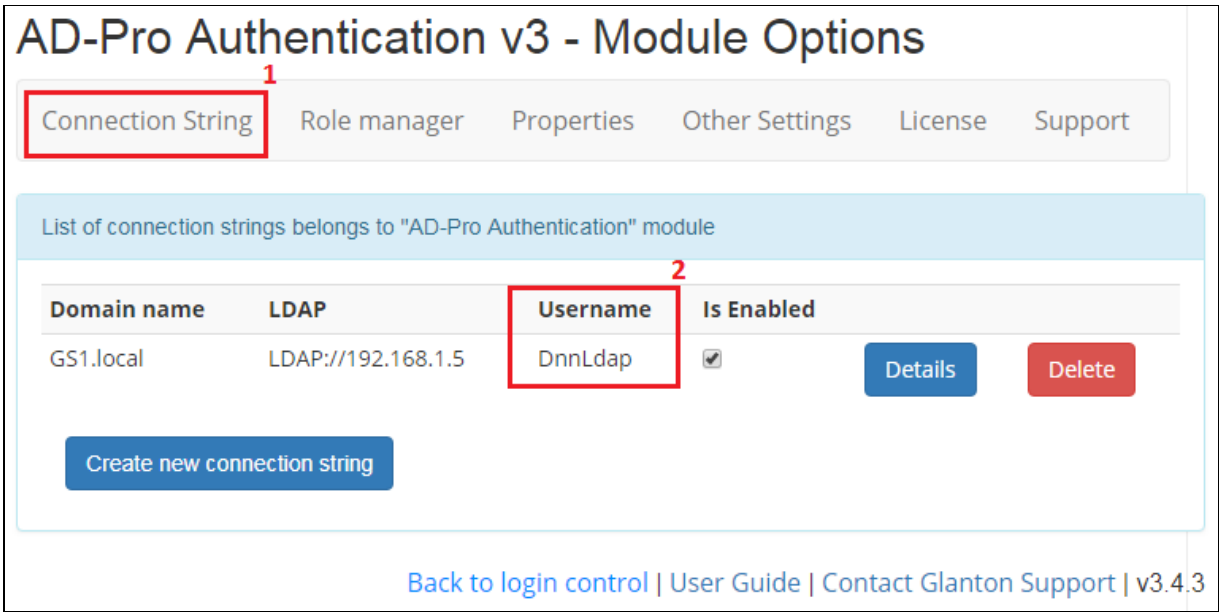


To set these permissions you can use following command executed under `Administrator` rights:

```
icacls c:\inetpub\vhosts\[DNN-SITENAME] /grant "IIS APPPOOL\[AppPoolNAME]":(OI)(CI)(M)
```

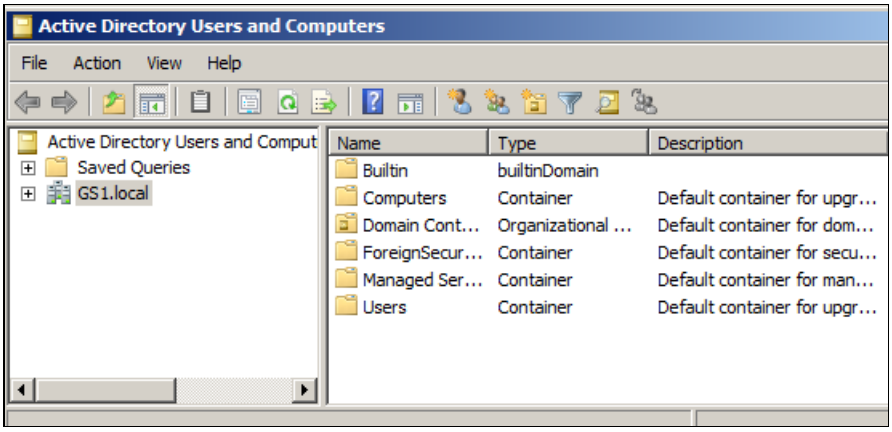
3.4. Initial AD configuration

The Active Directory user on behalf of which an LDAP connection is set up between DNN website and Active Directory system need to have special permissions. AD identity sepecified in “Connection String”, must have permissions to read AD groups, users, and user properties.

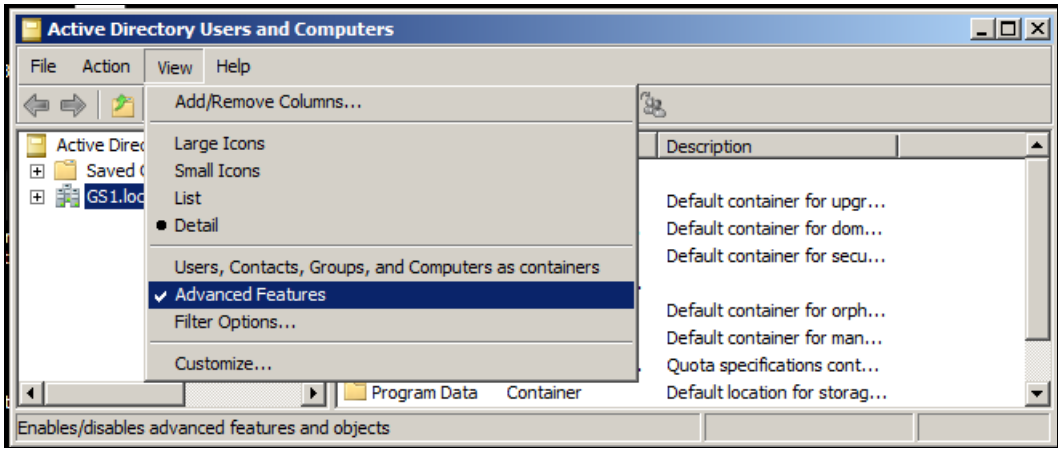


Below are the steps to set necesary permissions:

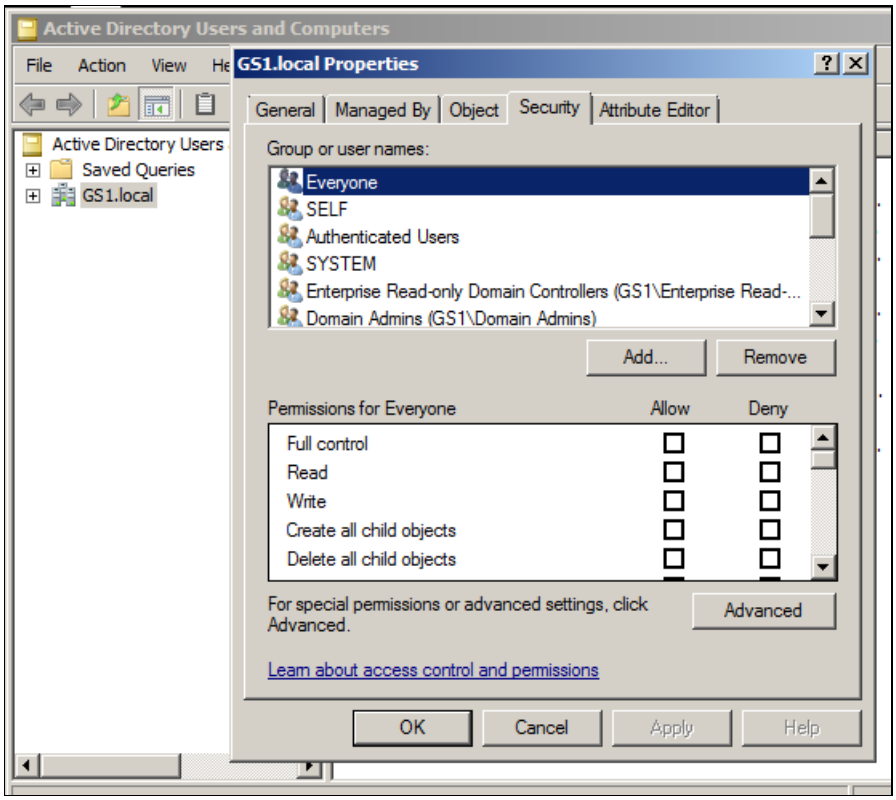
1. In Active Directory system, open the “Active Directory Users and Computers” window, see figure below.



2. Under “View” enable the “Advanced Features”, see figure below.

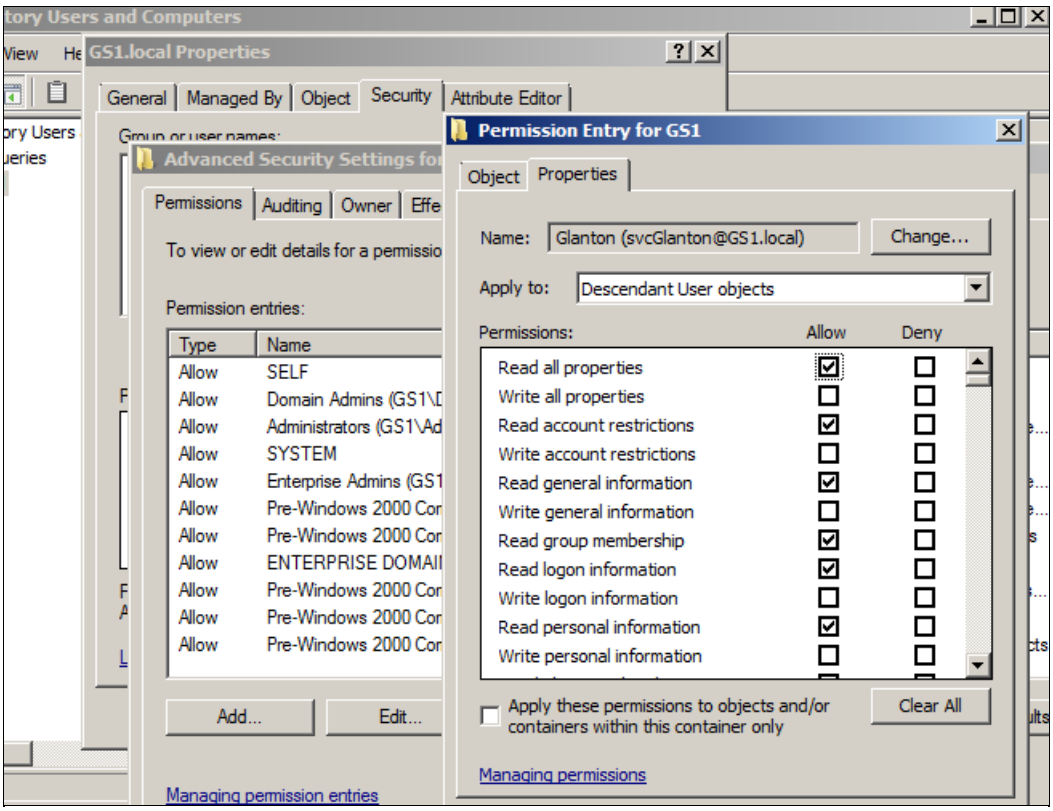


3. Right click on the “Domain” node and select the “Properties” from the context menu. Select the “Security” tab. And click on “Advanced” button, see figure below.



4. Click button “Add...” to add a user that is specified in “Module options-> Connection String”.

5. From the “Permission Entry” window select “Properties” tab. In “Apply to” select “Descendant Users object”. Make sure that following attributes are enabled: “Read all properties” and “Read Member Of”, see figure below.

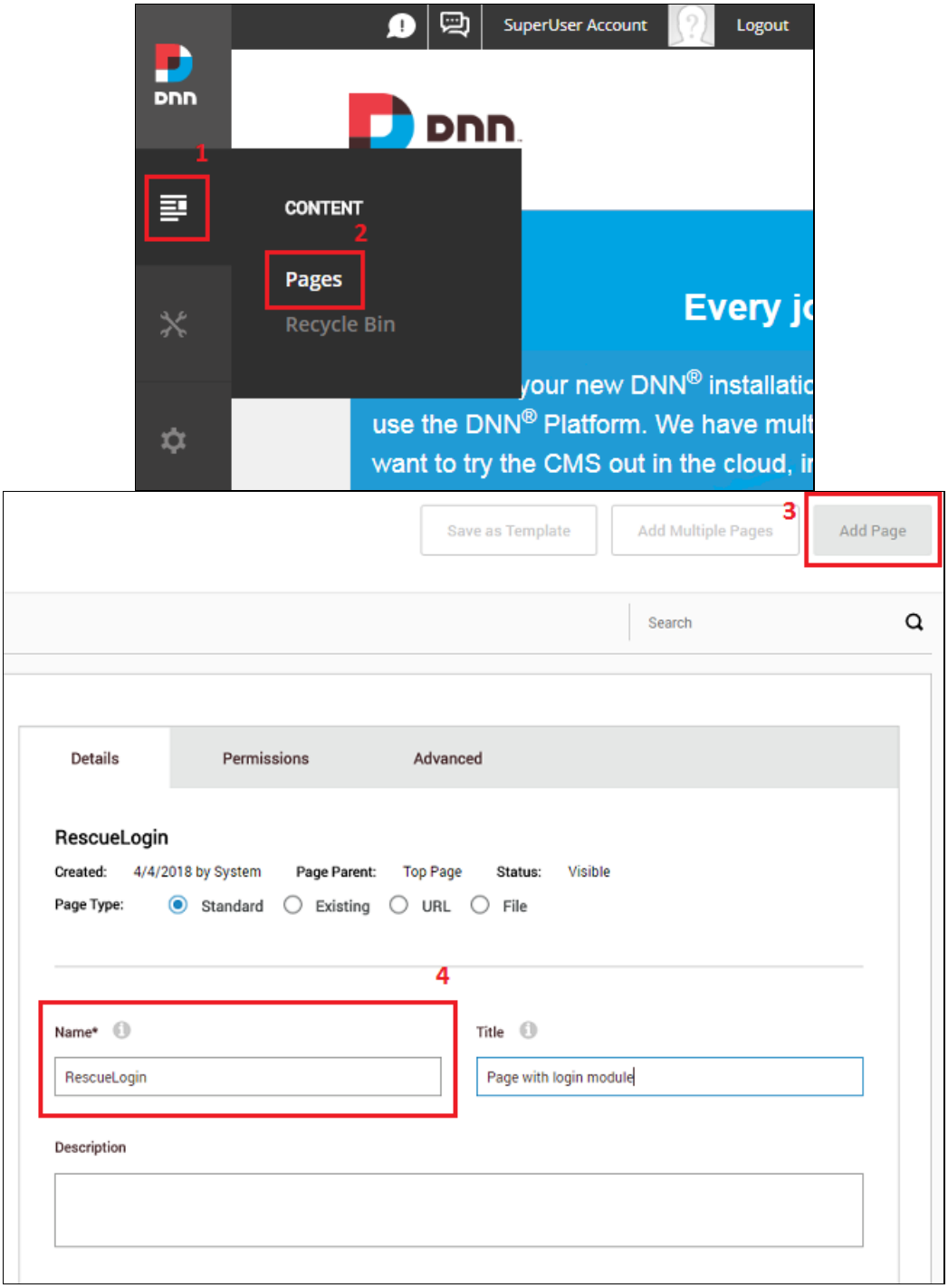


3.5. Rescue login

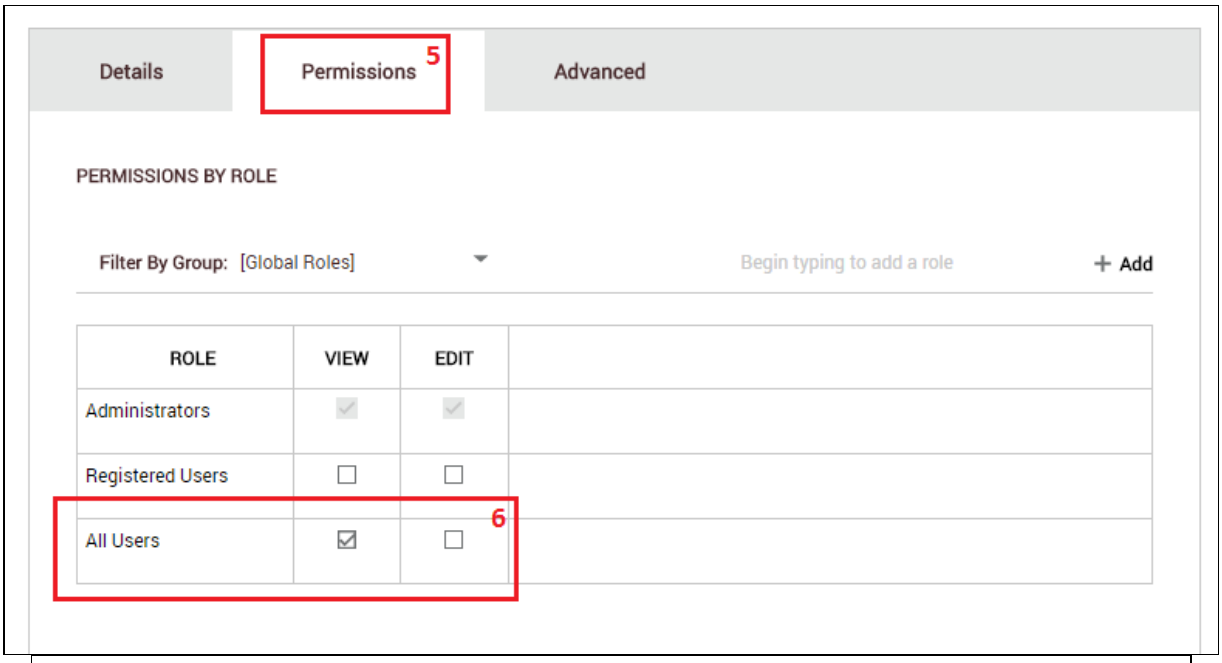
Note: Rescue login protect your DNN website against failures in ‘AD-Pro Authenitcation’ module.

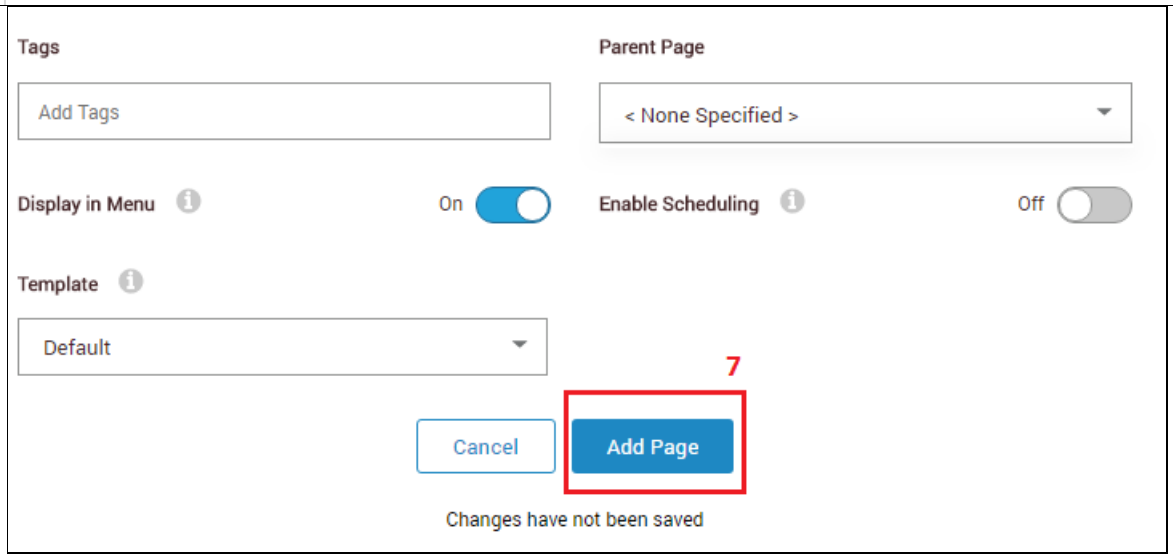
The login module has strategic importance for a website. If it fails you will not be able to sign in to DNN. Please execute steps below to create ‘Rescue Login’ page. This will allow you to sign in to DNN if something bad will happen.

1. Create new DNN page, see figures below.

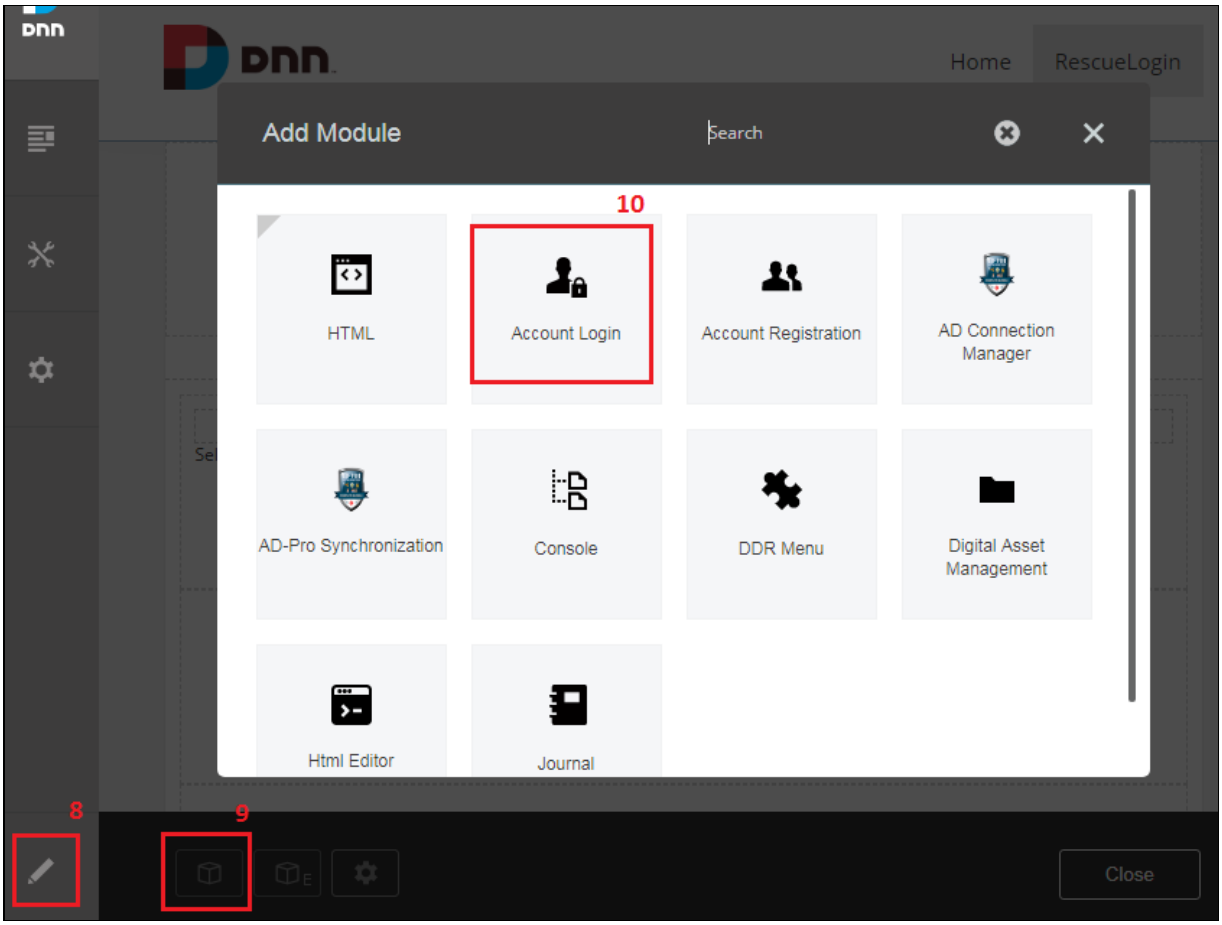


2. Set permission for that page 'View' for 'All users'. Click on 'Add Page' button to close wizard.

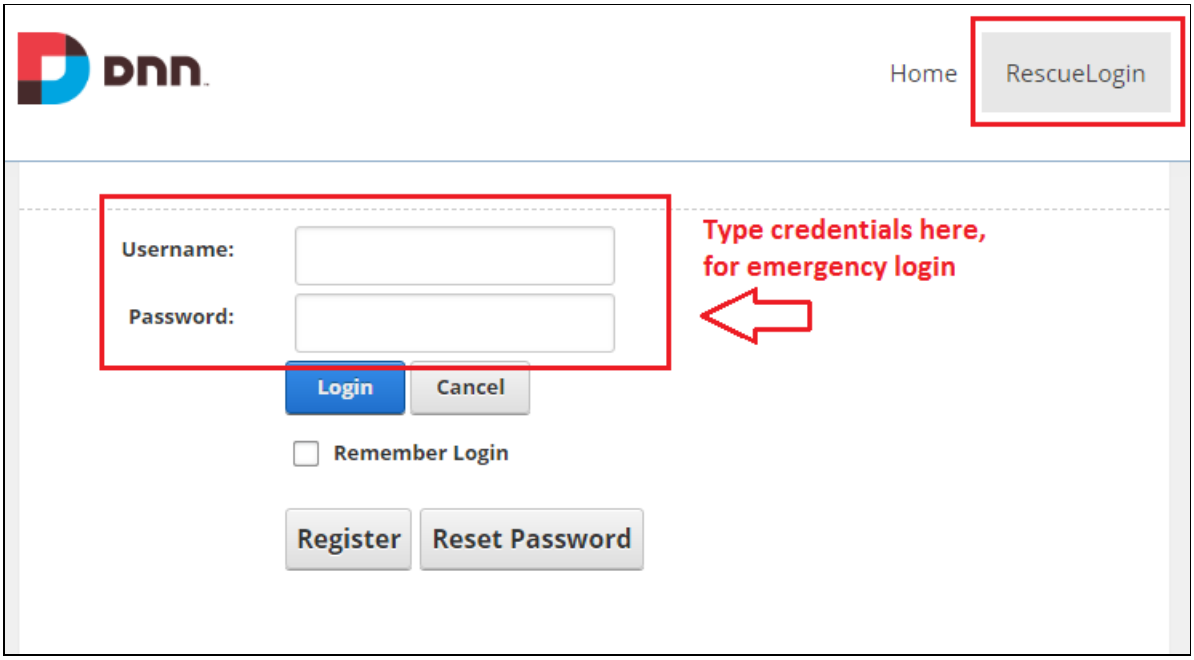




3. On newly created page put 'Account Login' module, see image below.



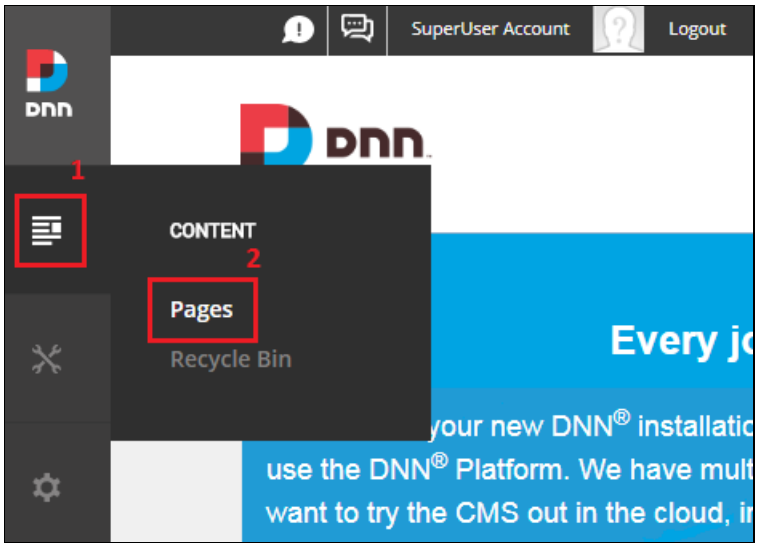
4. At the end you should have a page like on figure below. Sign in to DNN using this page, to test if it's working properly.



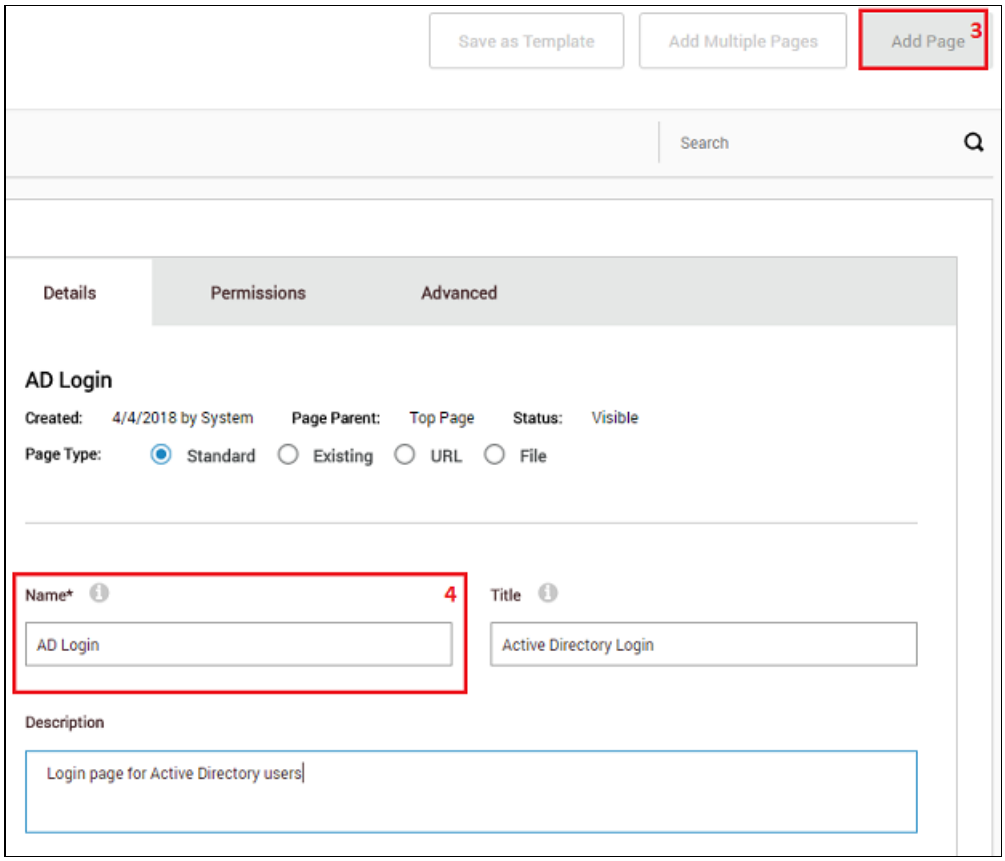
3.6. Dedicated login page

It's good to create dedicated page for the 'AD-Pro' login module. Please follow steps below to do that.

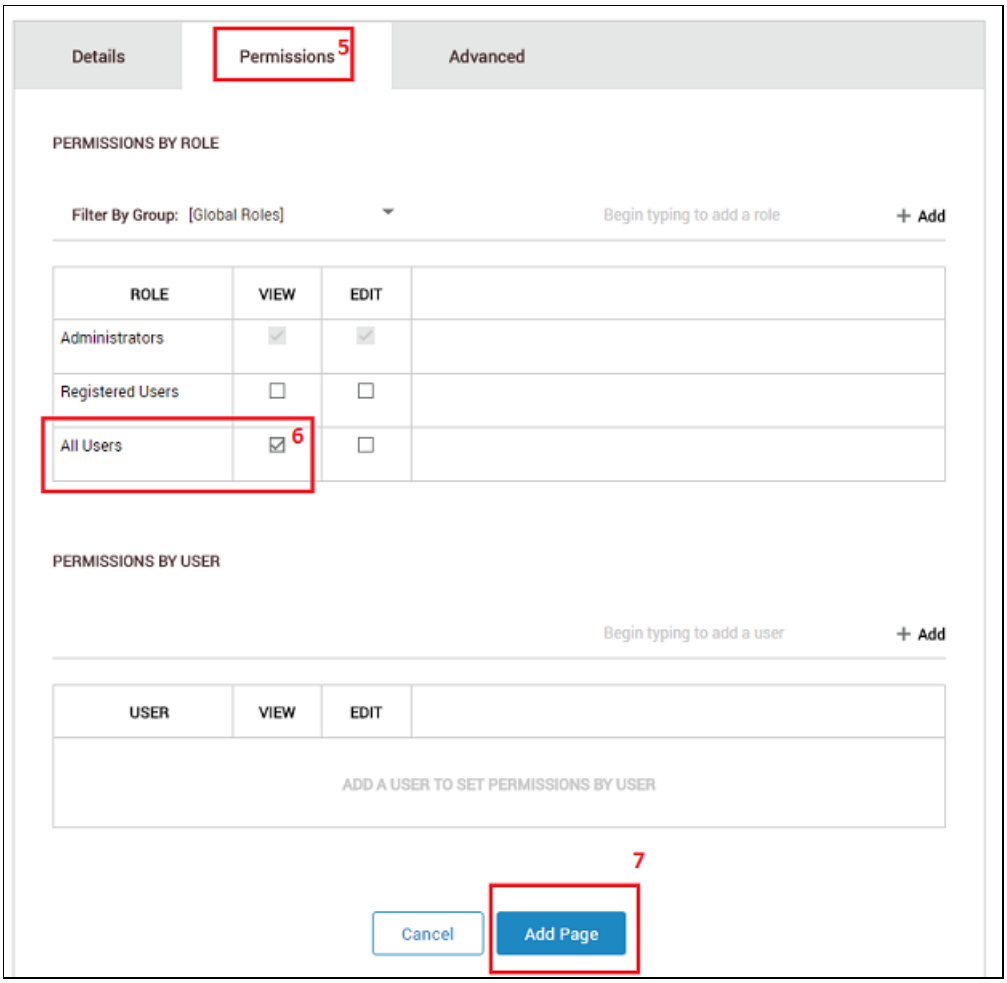
1. Sign in as DNN Administrator or Host, then select 'Pages' from the DNN menu to open the wizard, see figure below.



2. Click 'Add Page' and enter page name, see figure below.



3. It's very important to set correct permissions for the login page. Make sure that it's visible for 'All Users'. Then click 'Add page' to close the wizard. See figure below.

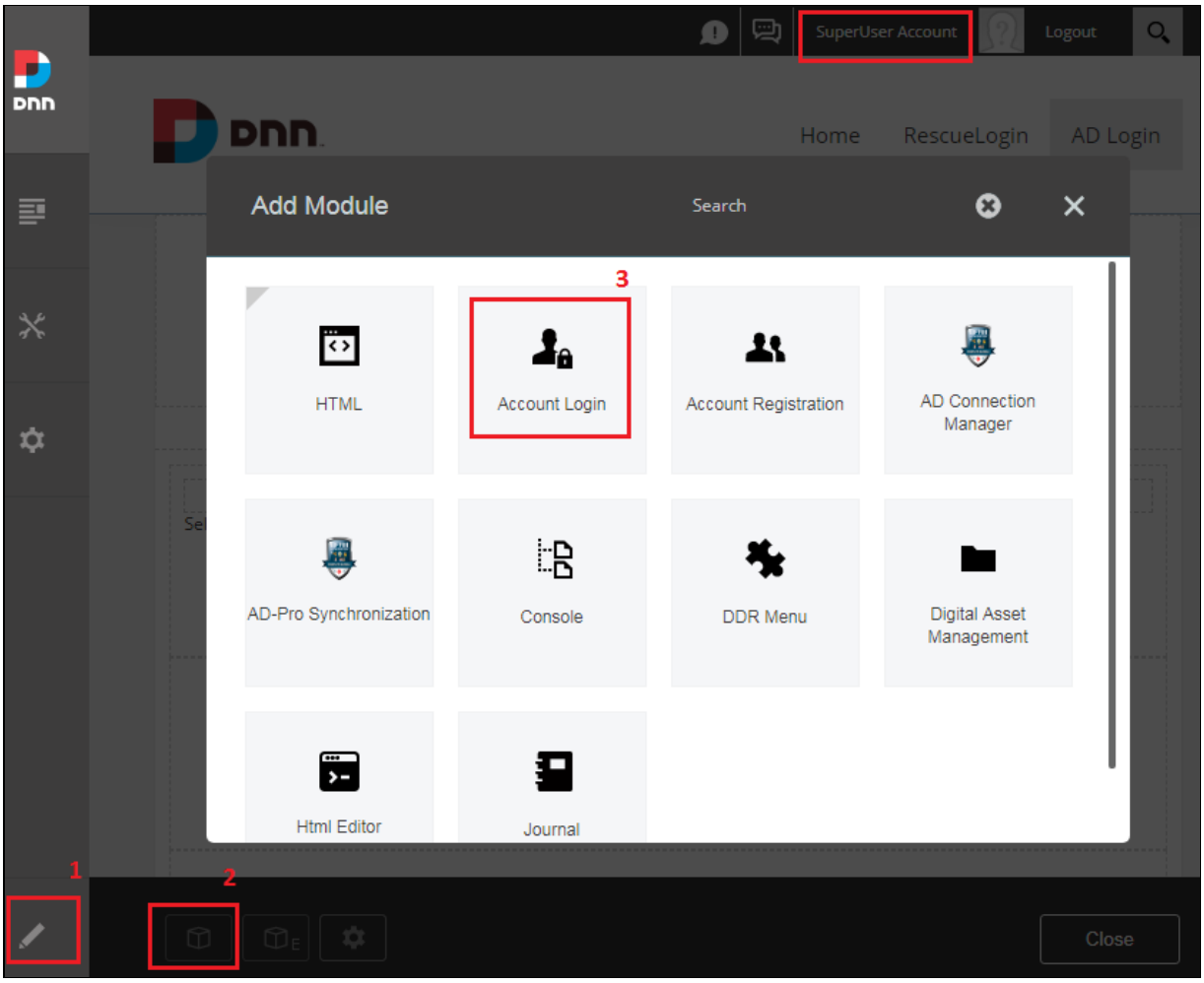


4. At the end, you should have new DNN page, where the login module will be putted. Page doesn't needs to be visible in the menu.

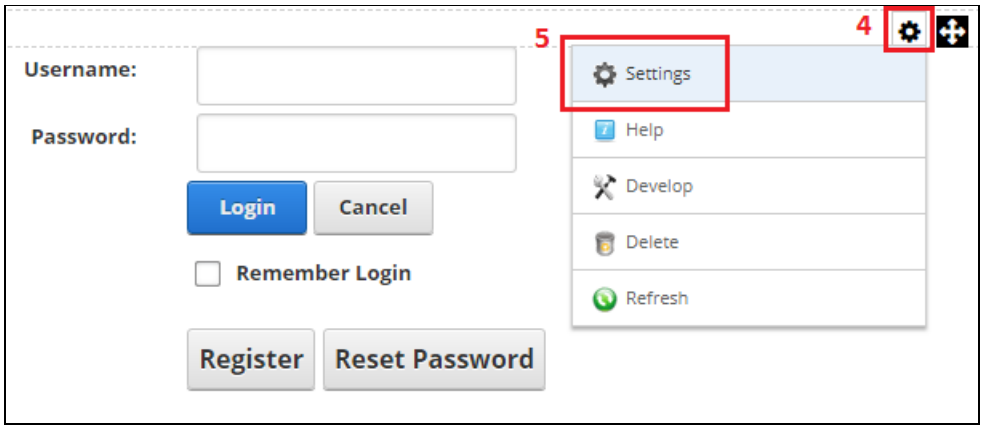
3.7. Add 'Account Login' module to a page

Login page needs to have core DNN login module, which is 'Account Login' module. It's important to set permissions for that module: 'View' only for 'Administrators'. Below are list of the steps to accomplish this task.

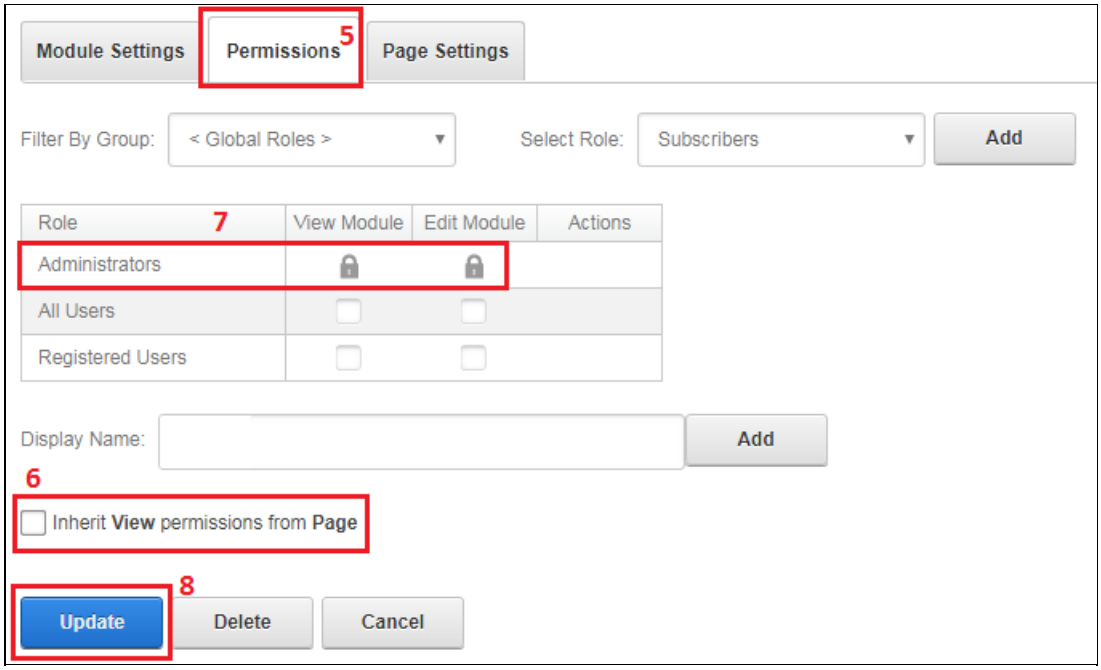
1. Sign in as DNN Administrator or Host, set DNN into 'Edit Mode' and put 'Account Login' module on a page, see figure below.



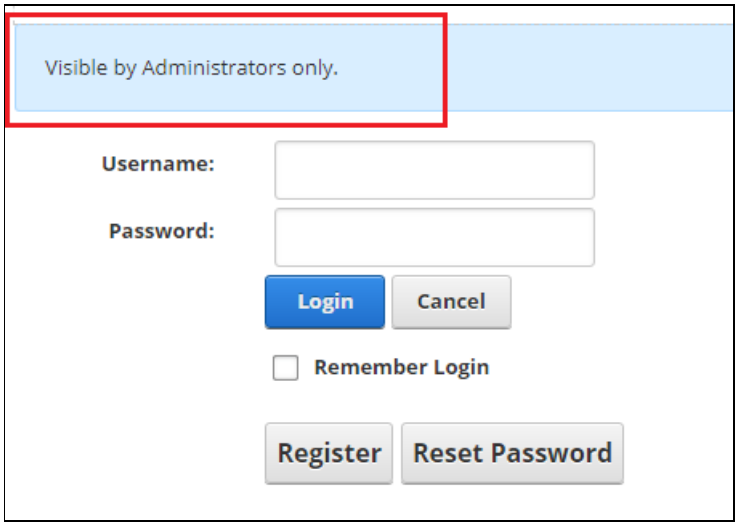
2. When the module is on a page, it's time to set permissions for it. Plugin needs to be visible only for 'Administrators'. Click on 'Gear' icon, then select 'Settings' from menu, see figure below.



3. Inside the module settings panel, select `Permissions` tab. Then make sure that `Inherit View permissions from Page` is disabled and module is visible only for 'Administrators'. If everything is set, click on `Update` button, see figure below for more info.

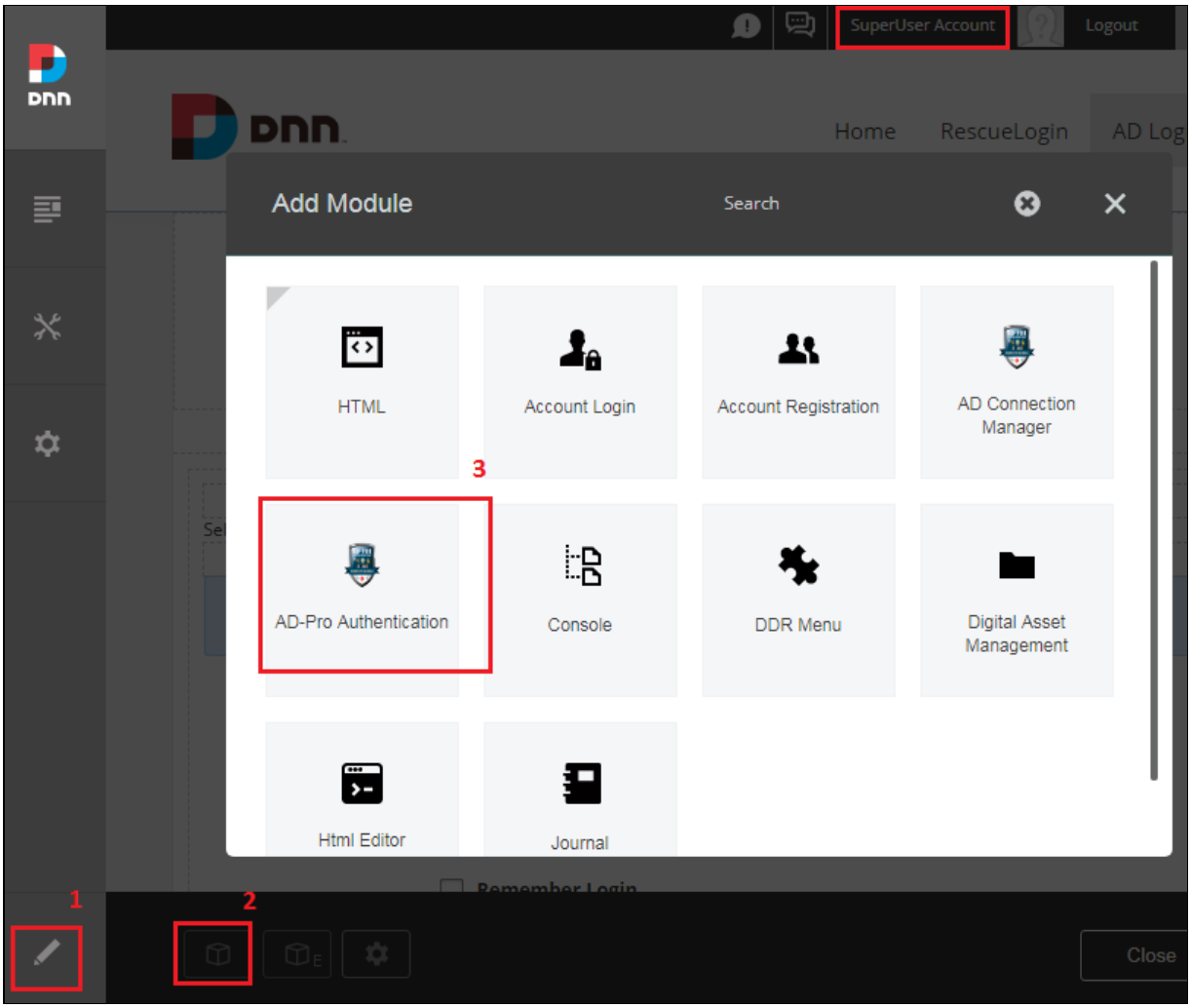


4. At the end of this step 'Account login' module will be displayed with new info at the top (blue background), see figure below.



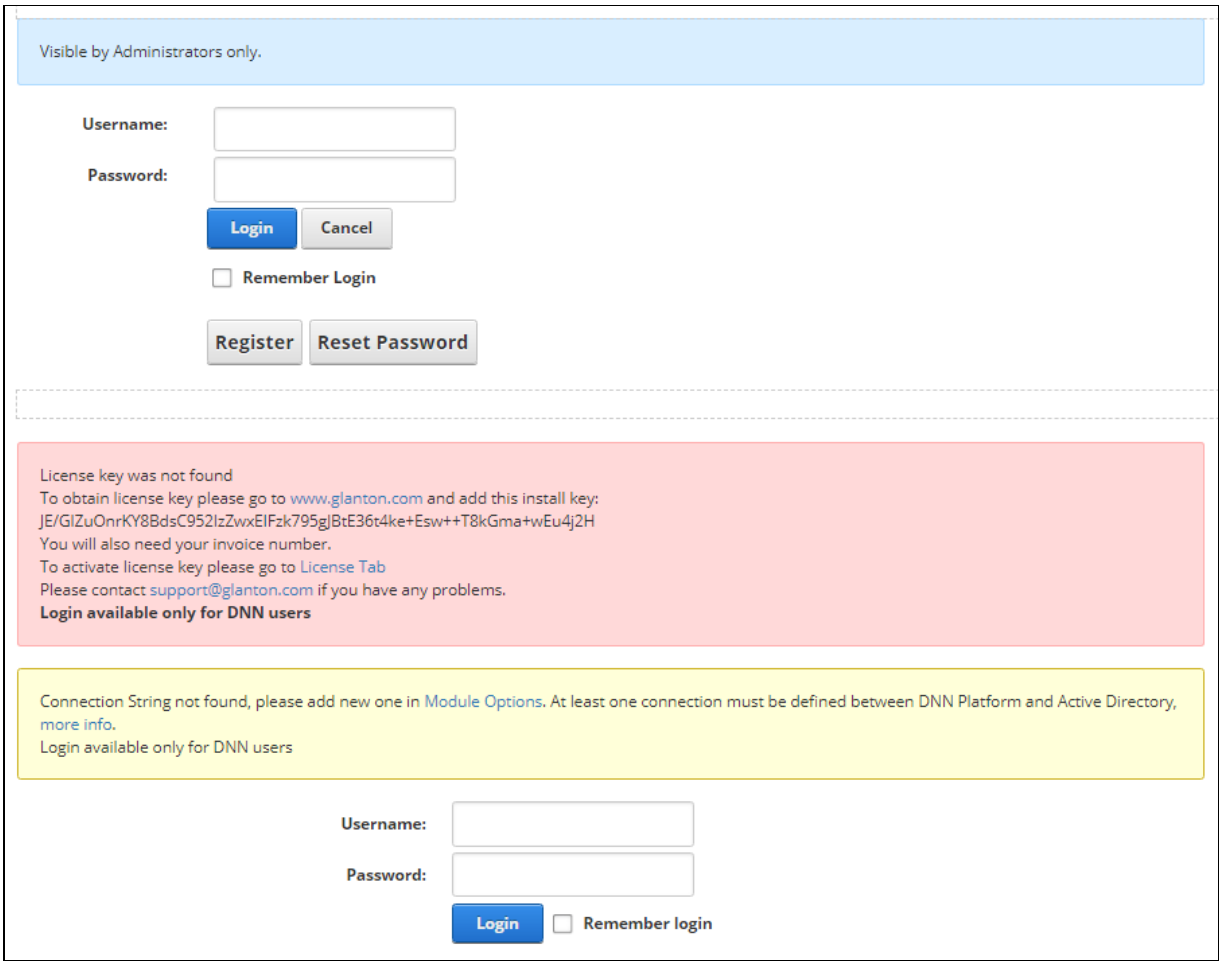
3.8. Add 'AD-Pro Authentication' module to a page

1. Sign in as DNN Administrator or Host, set DNN into 'Edit Mode' and put 'AD-Pro Authentication' module on a page, see figure below for details.



2. At the end of this process on one page should be two modules, like on figure below:

    - first 'Account Login' module (visible only for Administrators)
    - second 'AD-Pro Authentication' module (visible for all)



Now when both modules are on the page it's time to configure connection to the Active Directory system. This task is described in Configuring connection to Active Directory.

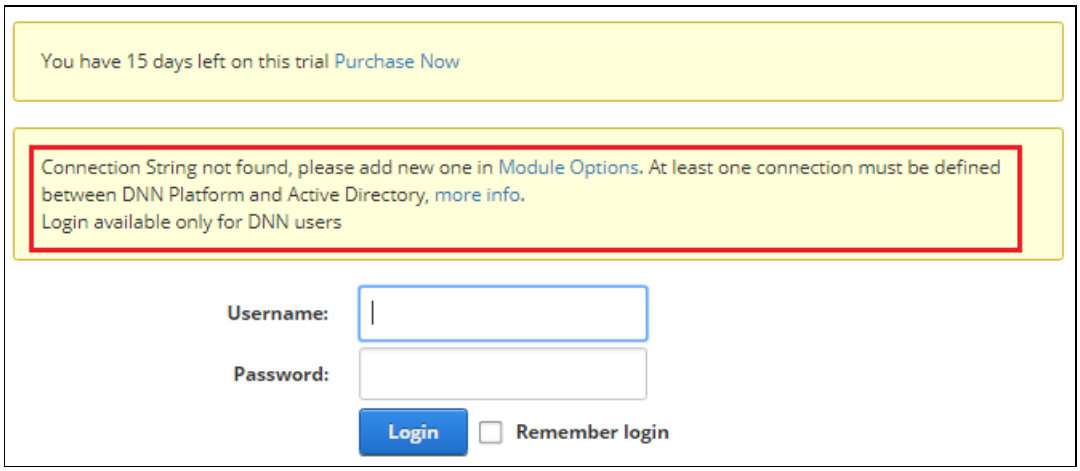
4. Configuring connection to Active Directory

Note: Objective of this chapter is to show how to set up connection between DNN Platform and Active Directory system.

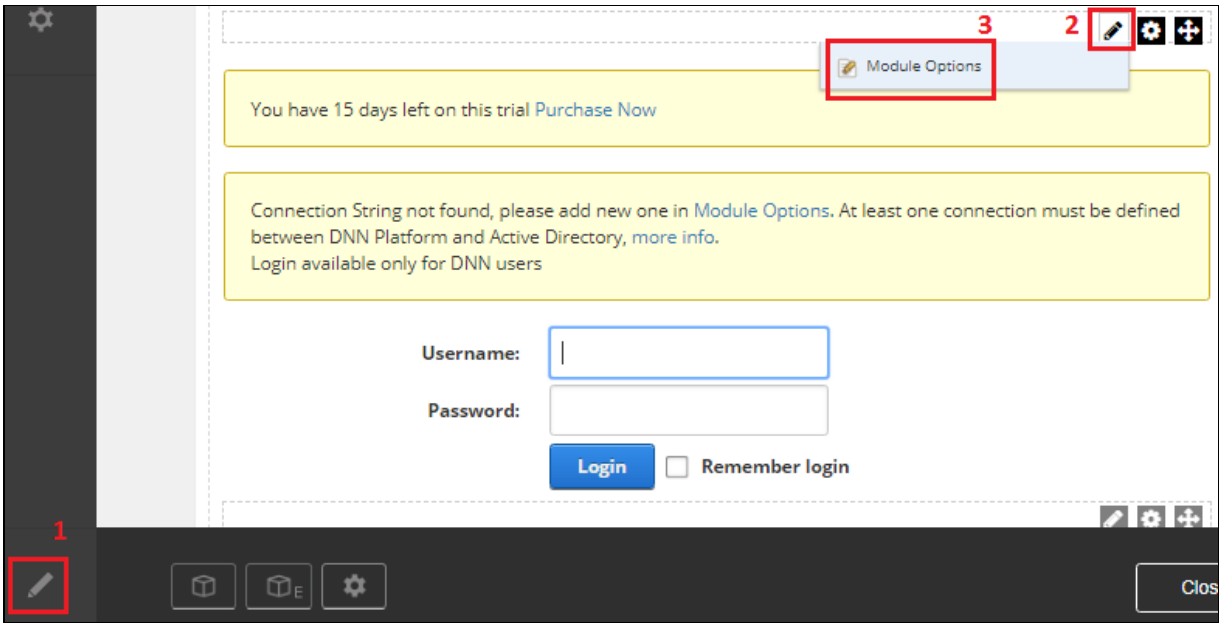
If you have never work with 'AD-Pro' plugin before, these steps are the most important to do.

1. Sign in to the DNN website as a 'DNN Host' or 'DNN Administrator'.

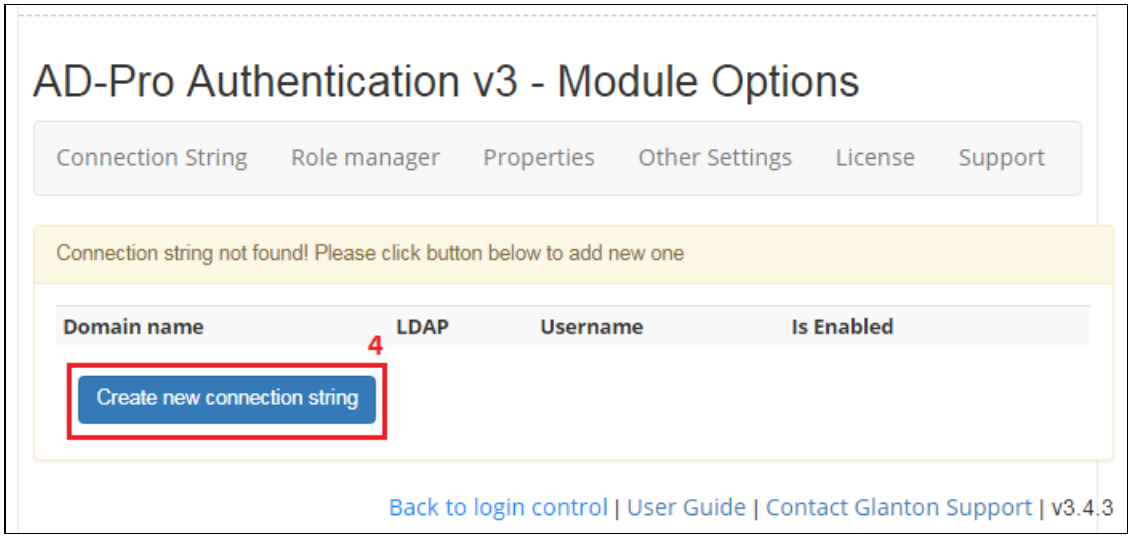
2. Go to page where 'AD-Pro Authentication' module is placed. If plugin doesn't have any connection defined, you should see message like on figure below. It informs you that module can't connect to Active Directory system, because it doesn't have any neccessary info to do that. Of course Active Directory login is not possible.



3. To set up new connection, first set DNN into 'Edit' mode, then go to 'Module Options', see figure below.

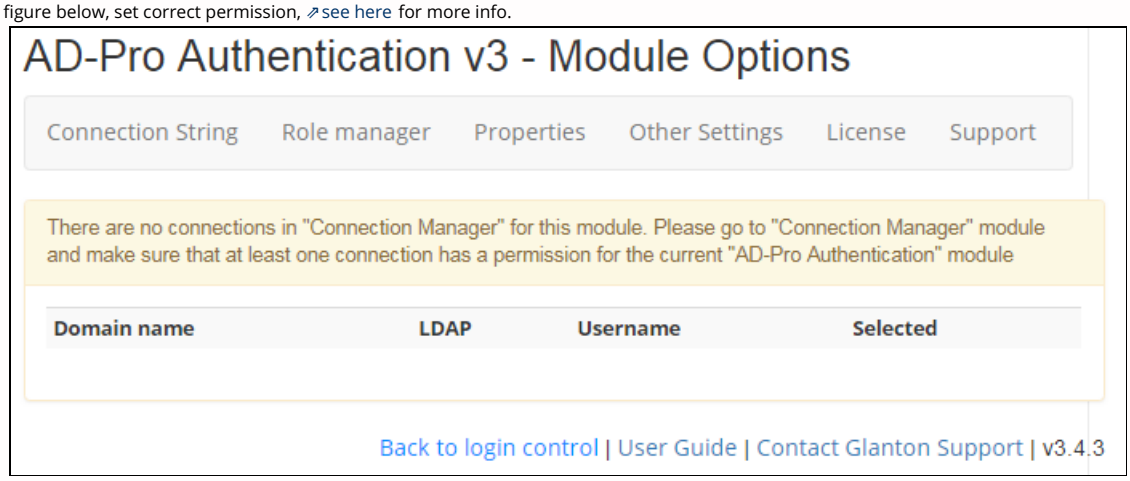


4. Under 'Connection String' tab, click on 'Create new connection string', see figure below.

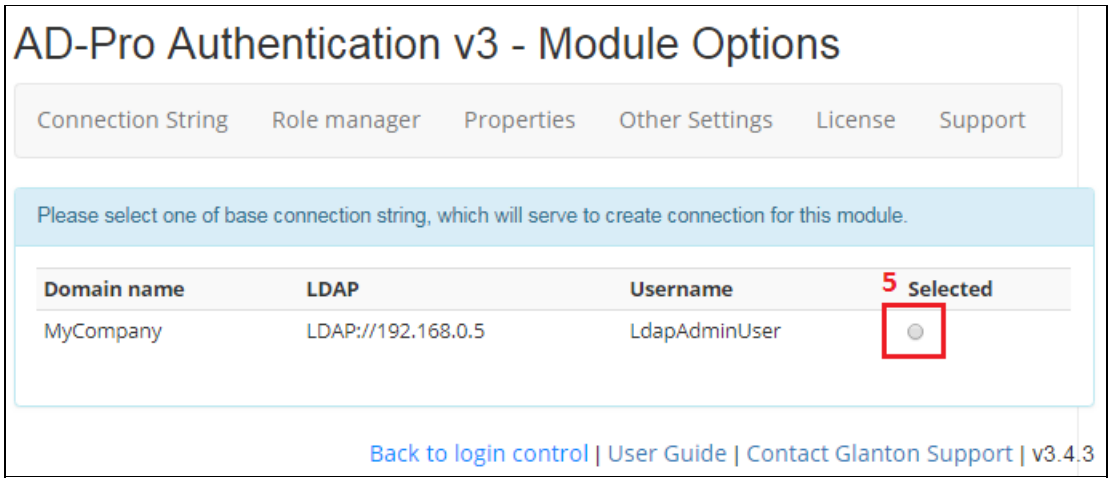


Warning

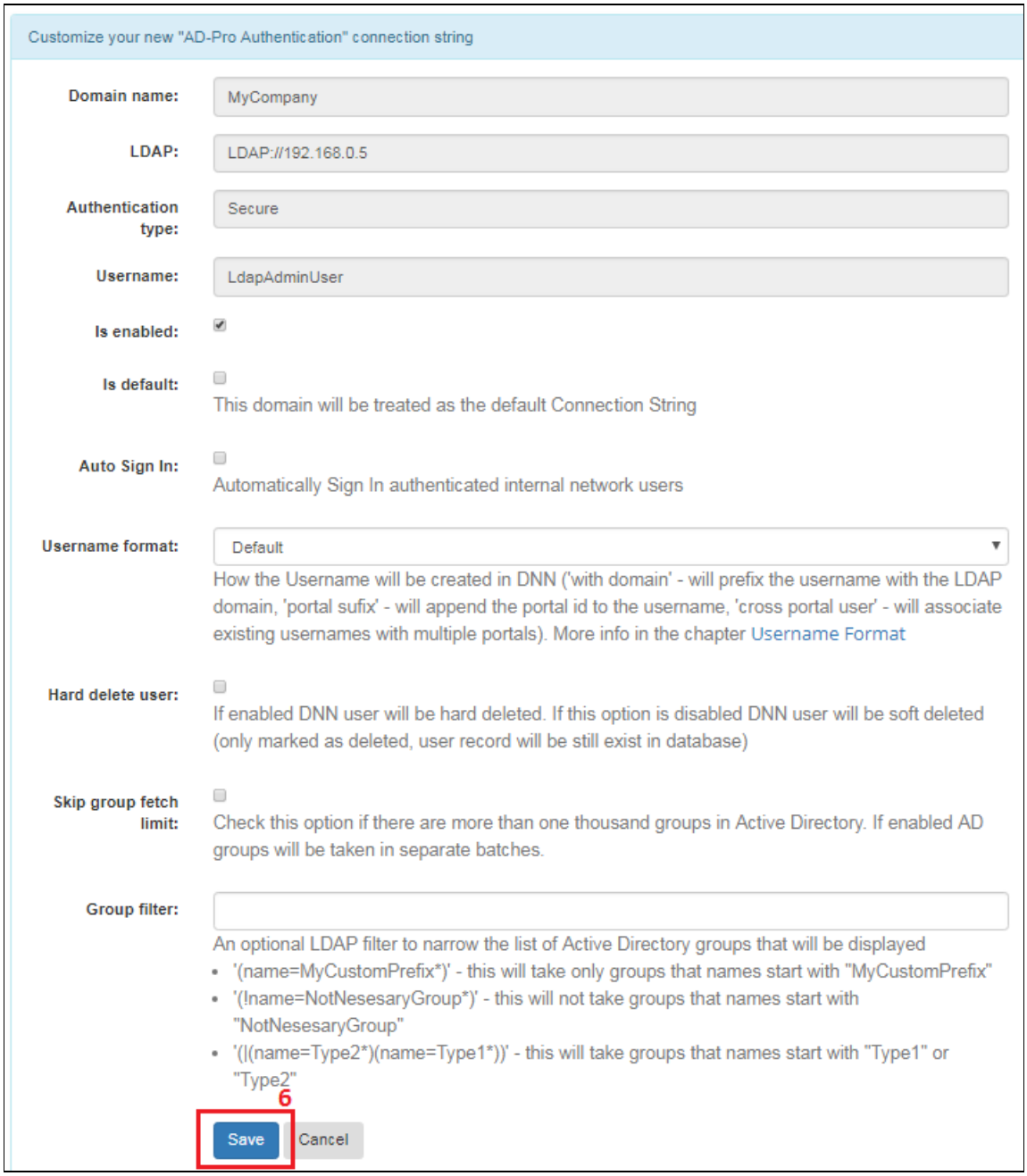
Please remember that at least one connection must have set permissions, to be visible from AD-Pro Authentication level. If you get message like on figure below, set correct permission, see here for more info.



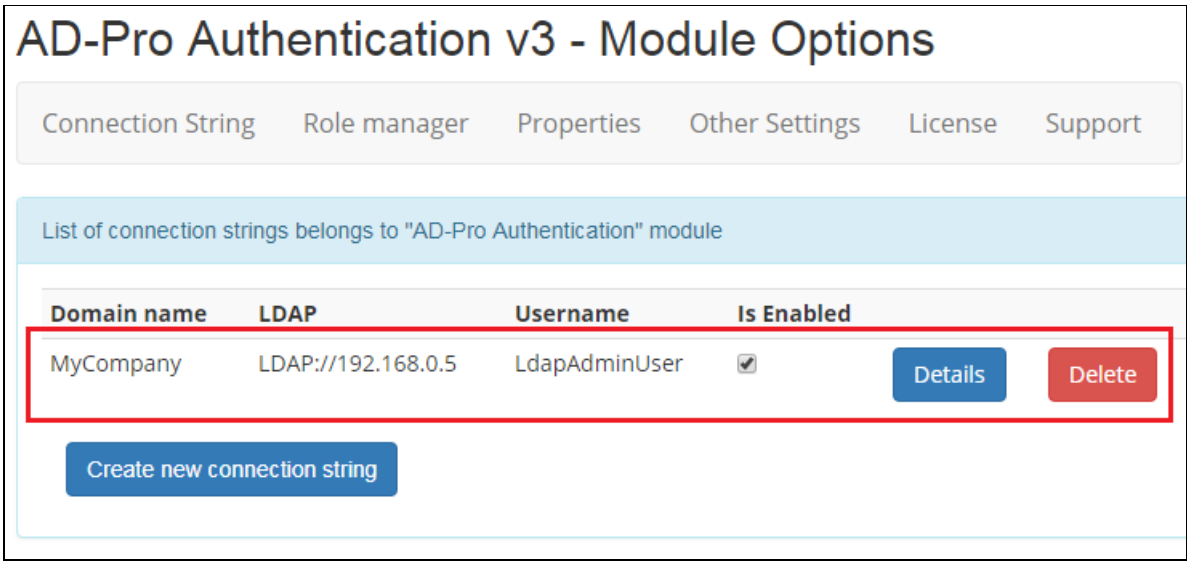
5. Select connection that you want to use, see figure below.



6. On this step leave all settings as it is, click on 'Save' button to finish wizard, see figure below.



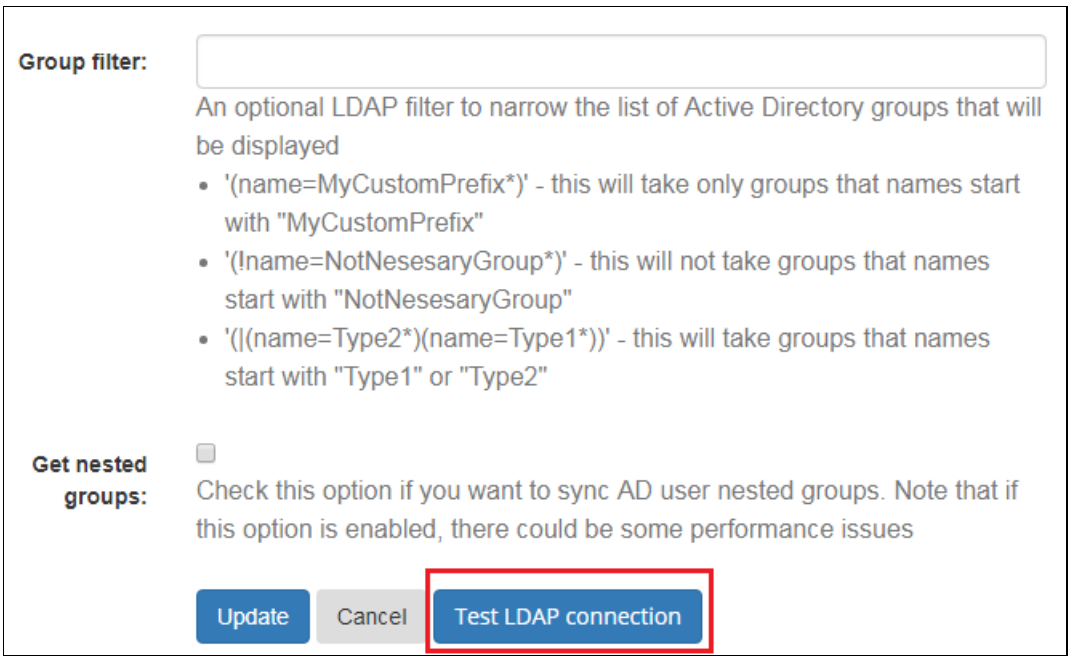
7. At the end, main screen should look like on figure below. The 'AD-Pro Authentication' module can connect to the Active Directory system.



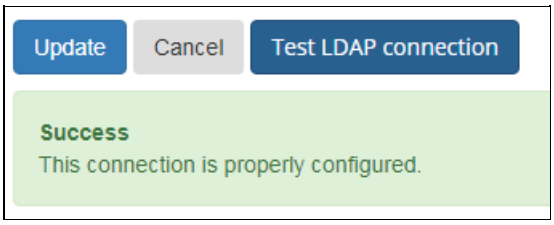
4.1. Validating connection

Note: This option is available in AD-Pro Authentication v4 or higher

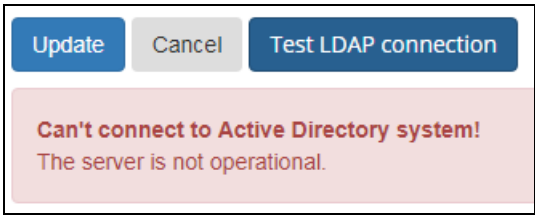
In easy way you can test connection between DNN and Active Directory. Each connection, under `Details` section has dedicated button `Test LDAP connection`, that can check LDAP, username, password and authentication type, see figure below.



If connection is properly configured, following meesage will be displayed.



or figure below if Active Directory system is not reachable



5. Role mapping

Note

Objective of this chapter is to show how:

- transfer Active Directory groups into DNN website
- restrict access to the AD login for uses from specified AD groups

5.1. Overview

The 'AD-Pro Authentication' plugin allows push Active Directory groups to the DNN website, in other words an AD user can have the same groups as corresponding DNN user. This significantly improves user managemant tasks. For example access to DNN page can be restricted only for specified AD groups. Now **from Active Directory level** we can decide if user can get access to DNN page.

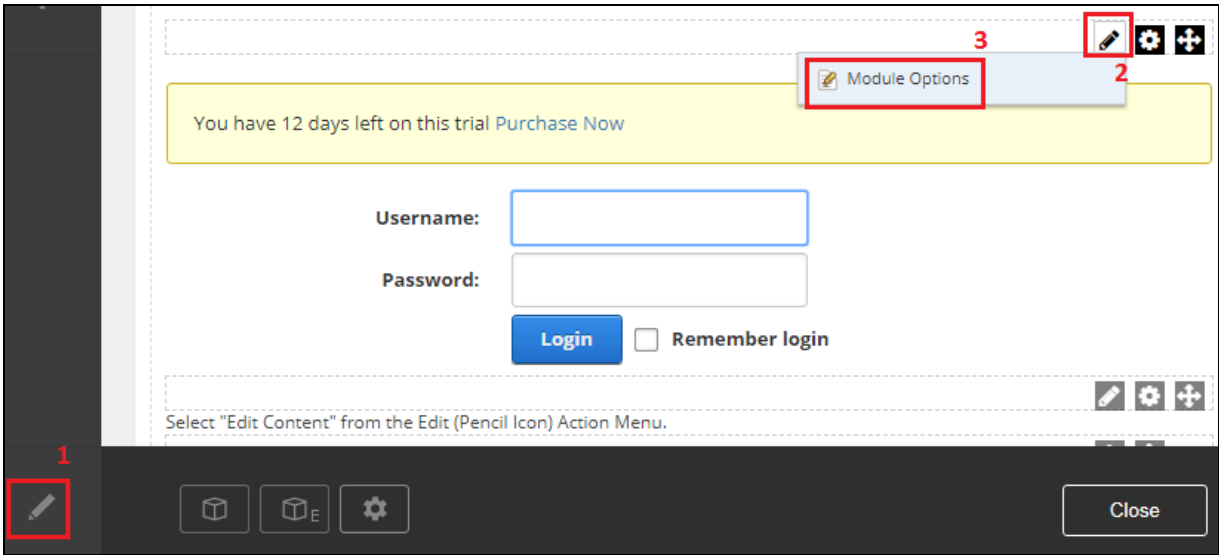
Additionally 'AD-Pro Authentication' plugin can allow sign in only users from a specified Active Directory group(s). For example only users belongs to AD group 'Students' are able to sign in to DNN website.

Note: To work with 'Role mapping manager' first a valid connection to Active Directory needs to be set, see Configuring connection to Active Directory chapter for more info.

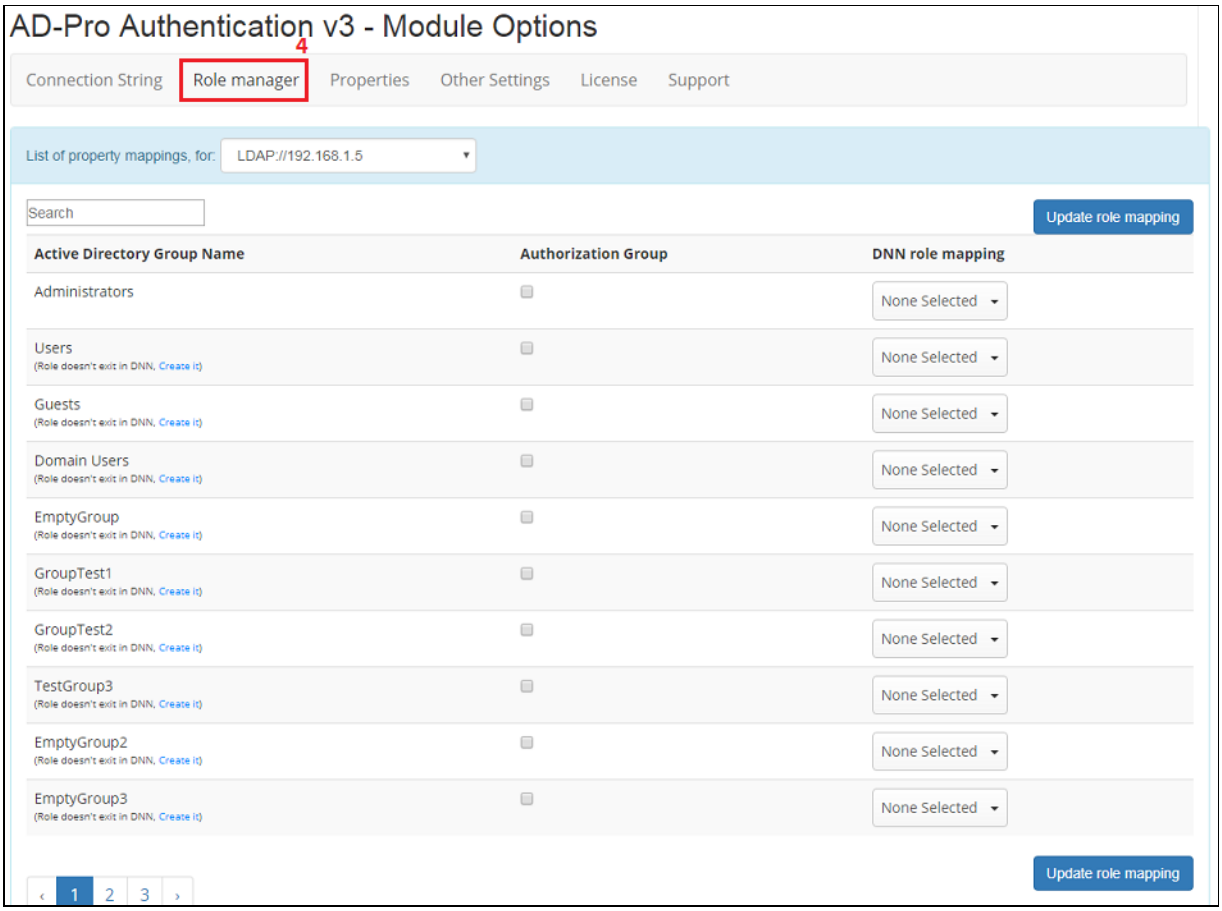
5.2. Transfering AD groups to DNN

As already beed said, 'AD-Pro Authentication' can push AD group to DNN. What is important, it what happens only at sign in process. When the role is transfered to DNN, it can have same name as AD group or, using a special mapping, AD group can be connected with any DNN role. It's even possible to connect one AD group with multiple DNN roles. Below are configuration steps that needs to be done to transfer AD group `GroupTest1` to DNN.

1. First sign in to DNN website as a 'DNN Host' or 'DNN Administrator'.
2. Go to page where 'AD-Pro Authentication' module is placed.
3. Set DNN into 'Edit' mode, then go to 'Module Options', see figure below.

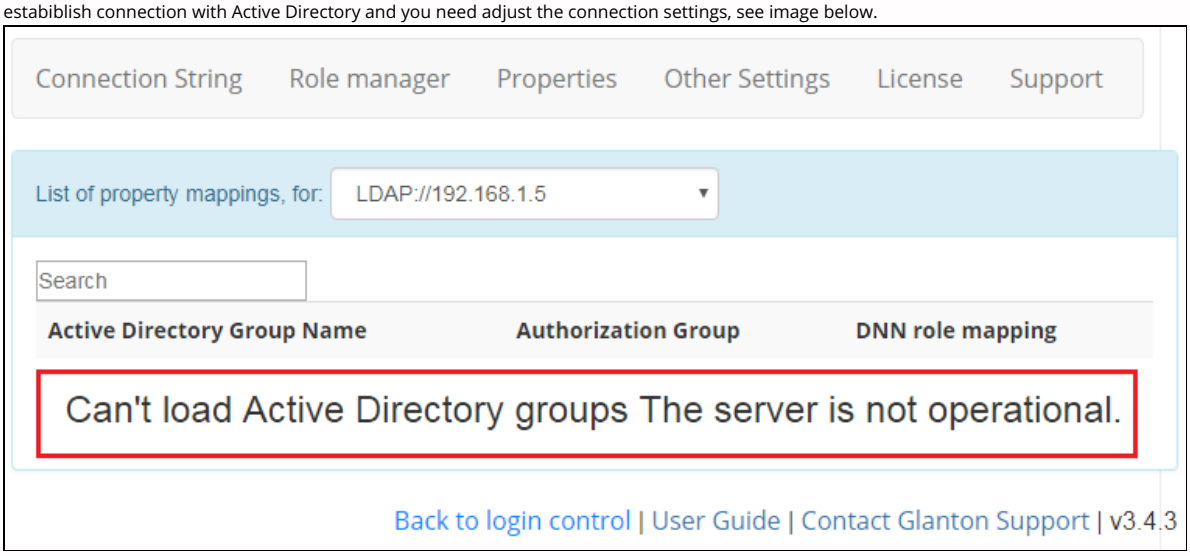


4. Go to 'Role Manager' tab where Active Directory groups should be listed, see image below.

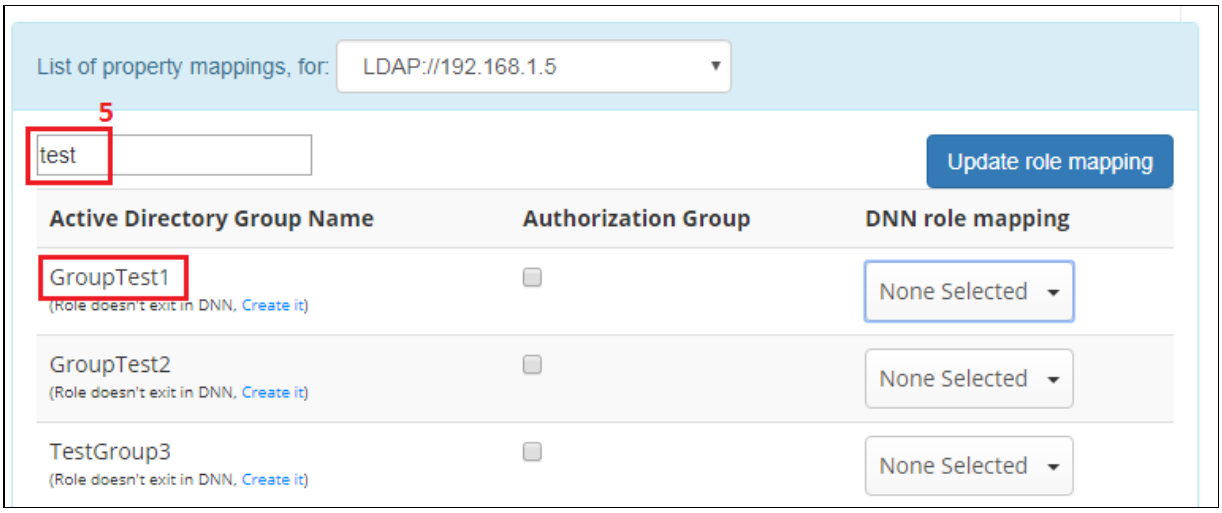


Warning

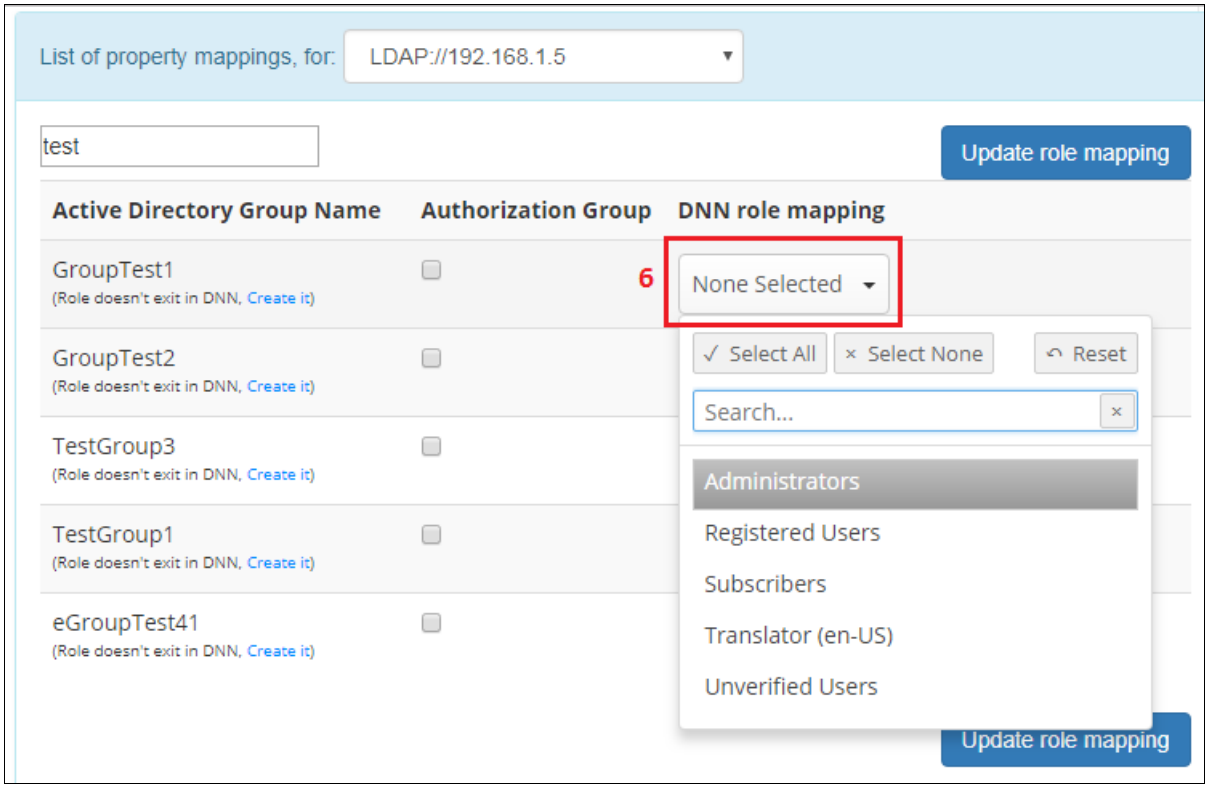
If 'Role Manager' tab displays message like: *Can't load Active Directory groups The server is not operational*, this means that DNN is unable to estabiblish connection with Active Directory and you need adjust the connection settings, see image below.



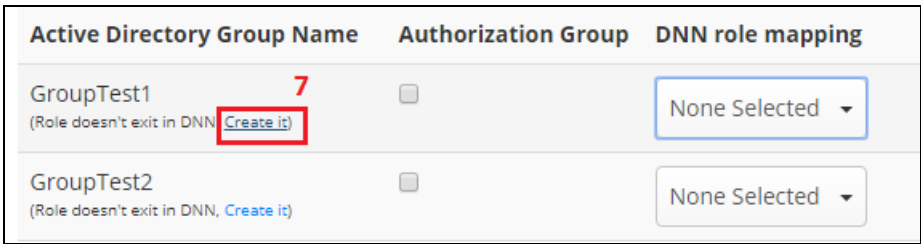
5. In the filter box enter group name, this will narrow list of the displayed groups, see image below.



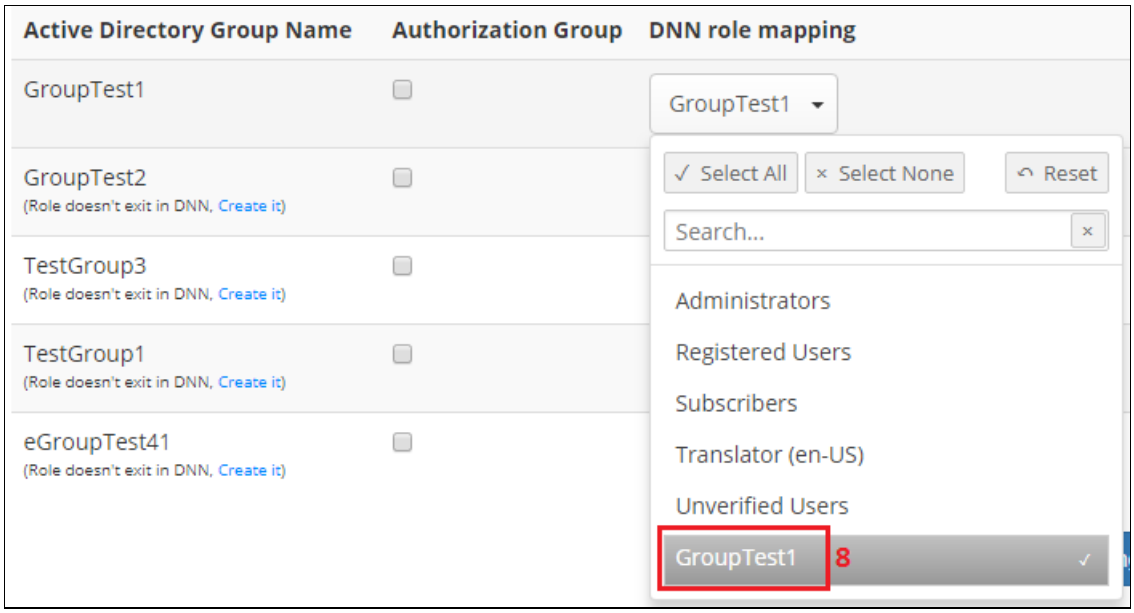
6. Set one or more corresponding DNN roles from 'DNN role mapping' column, see image below.



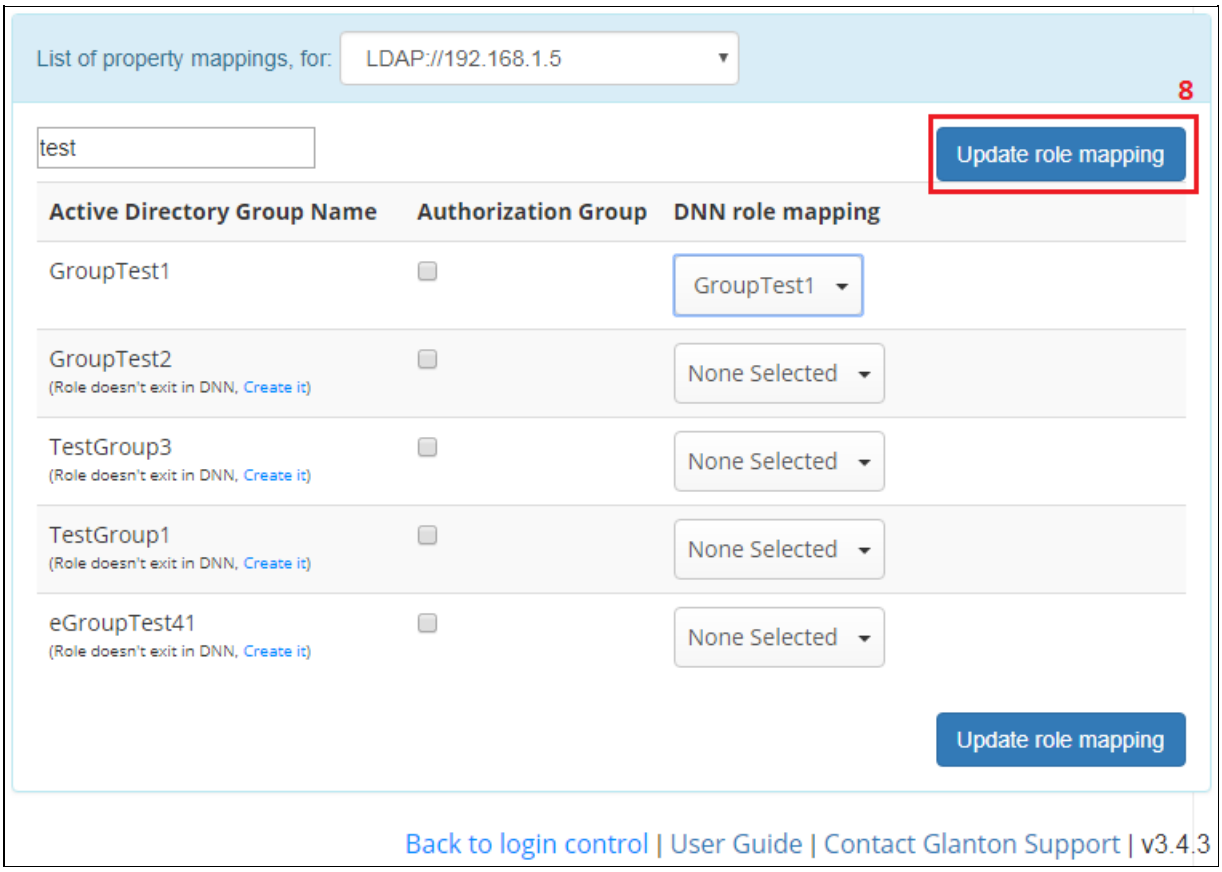
7. We want set mapping from AD group 'GroupTest1' to DNN role 'GroupTest1', but that group doesn't exist in DNN yet. Click on `Create it` link to create 'GroupTest1' in DNN, see image below.



8. Now we can easily set mapping from AD group 'GroupTest1' to DNN role 'GroupTest1', see image below. Please notice that `Create it` link no longer exist.



9. Click on 'Update role mapping' to save the changes, see image below.

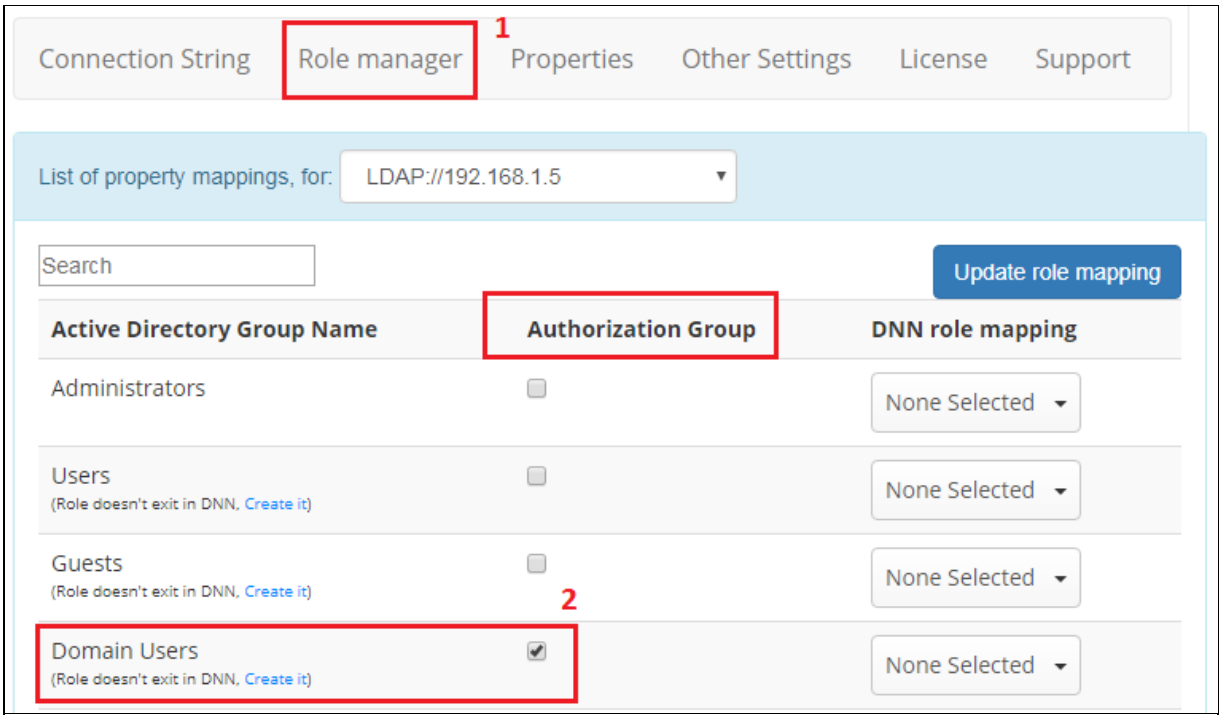


Task is completed. Now AD user that belongs to group 'GroupTest1', will have the same role in DNN, please remember that this will happen on next login process.

5.3. Allow logon for all Active Directory users

In easy way you can open access to DNN website for all Active Directory users. Please notice that all AD users are members of group 'Domain Users', therefore setting this group as a authorization group, will open DNN for all users.

To do that please go to 'AD-Pro Authentication-> Module options-> Role Manager' tab, and for role 'Domain Users' enable checkbox under 'Authorization' column. Now all AD users can sign in to DNN. See figure below for more details.



5.4. Restrict logons to a group of users

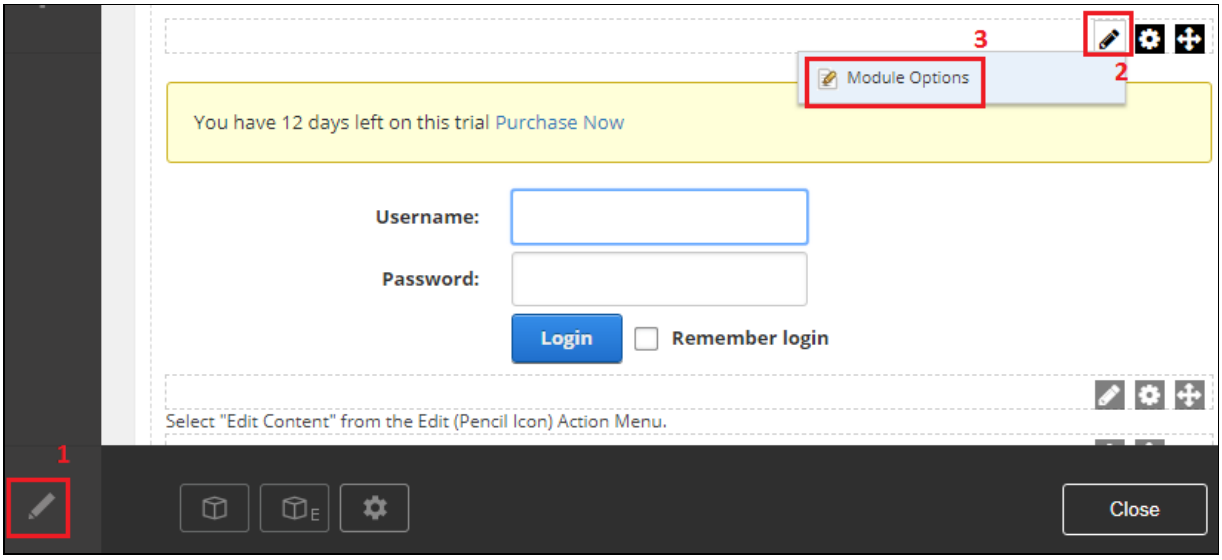
The 'AD-Pro Authentication' module allows you to limit Active Directory users that are able to sign in to DNN. This can be done through 'Role manager' and column 'Authorization Group'. Below are simple steps that needs to be done to allow all AD users to sign in to DNN. We will utilize AD group 'Domain Users', to which by default all AD users are assigned.

Important: At least one Active Directory group needs to be enabled inside 'Authorization Group' column. In other case all AD users will be rejected from the logon.

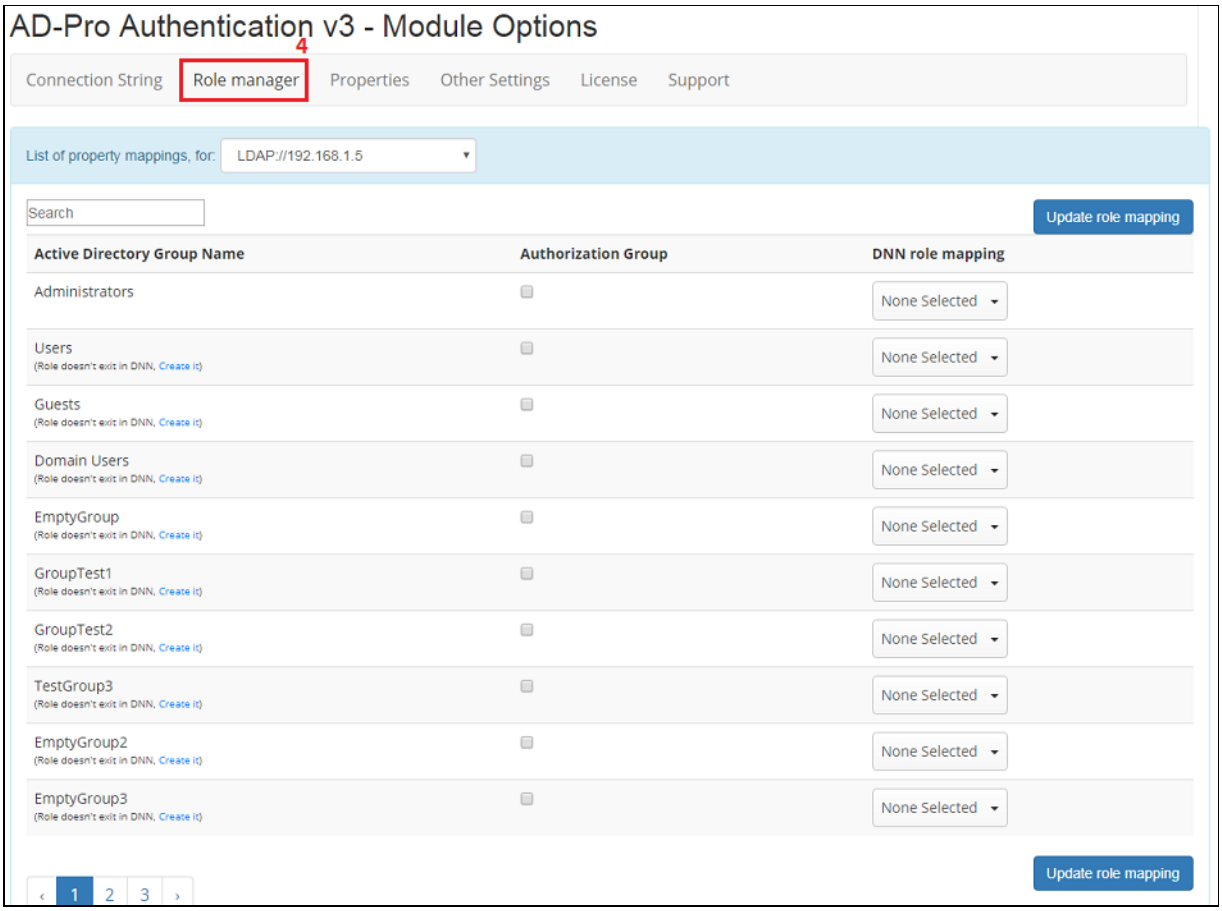
1. First sign in to DNN website as a 'DNN Host' or 'DNN Administrator'.

2. Go to page where 'AD-Pro Authentication' module is placed.

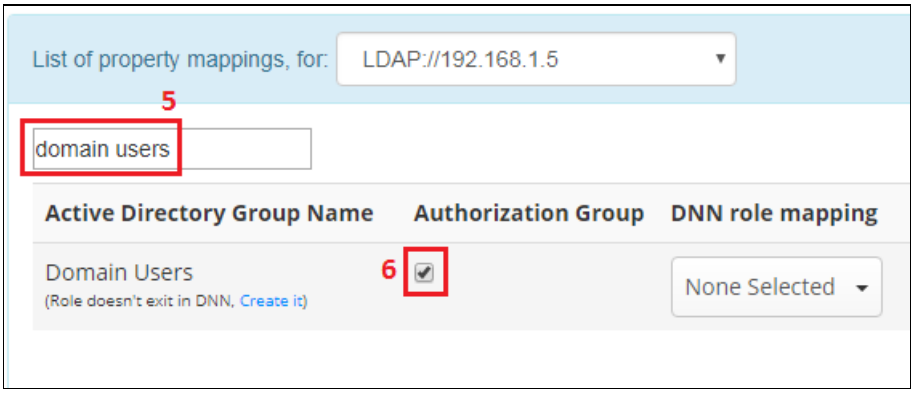
3. Set DNN into 'Edit' mode, then go to 'Module Options', see figure below.



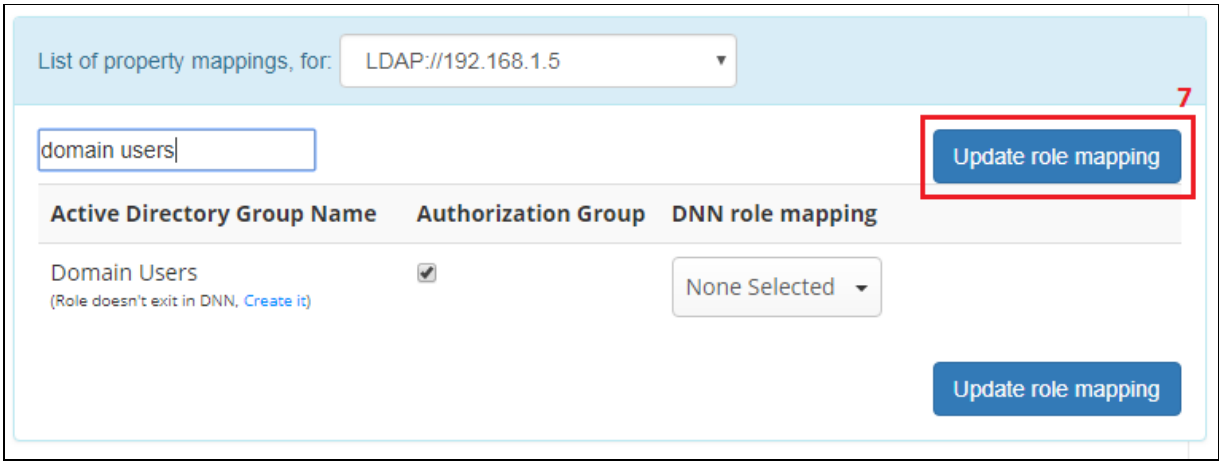
4. Go to 'Role Manager' tab where Active Directory groups should be listed, see image below.



5. Find 'Domain Users' group (for simplify put 'domain users' string inside filter box), then tick chckbox, see image below.



6. Click on 'Update role mapping' button, to save the changes, see image below.



Task is completed. Now all Active Directory users will be able to sign in to DNN website, through the 'AD-Pro Authentication' plugin.

5.5. Revoking user from a role

The “AD-Pro Authentication” can unassign DNN user from a DNN role, only if:

- the login process is happening,
- corresponding AD user doesn’t belong to specified AD group,
- AD group has a mapping in the “AD-Pro Authentication->Role Manager”,

Consider following scenario where we have:

- Active Directory user: “AD\Bob”,
- Active Directory group “Role_1”,
- DNN user “Bob”,
- DNN role “Role_1”;

Now let’s say that:

- DNN user “bob” was manually assigned to the DNN role “Role_1”,
- corresponding AD user “AD\Bob” doesn’t belongs to AD group “Role_1”,
- in “AD-Pro Authentication” in “Role Manager” following mapping is created: if AD user belongs to AD group “Role_1”, add to the corresponding DNN user role “Role_1”,

Now user “AD\Bob” is trying to login to DNN using “AD-Pro Authentication” module. And at the login process DNN user “Bob” is removed from DNN role “Role_1”. It’s because “Role_1” has a mapping in “Role Manager” and AD user “AD\Bob” doesn’t belong to AD group “Role_1”.

6. Profile mapping

> **Note:** Objective of this chapter is to show how transfer Active Directory user profile into DNN.

6.1. Overview

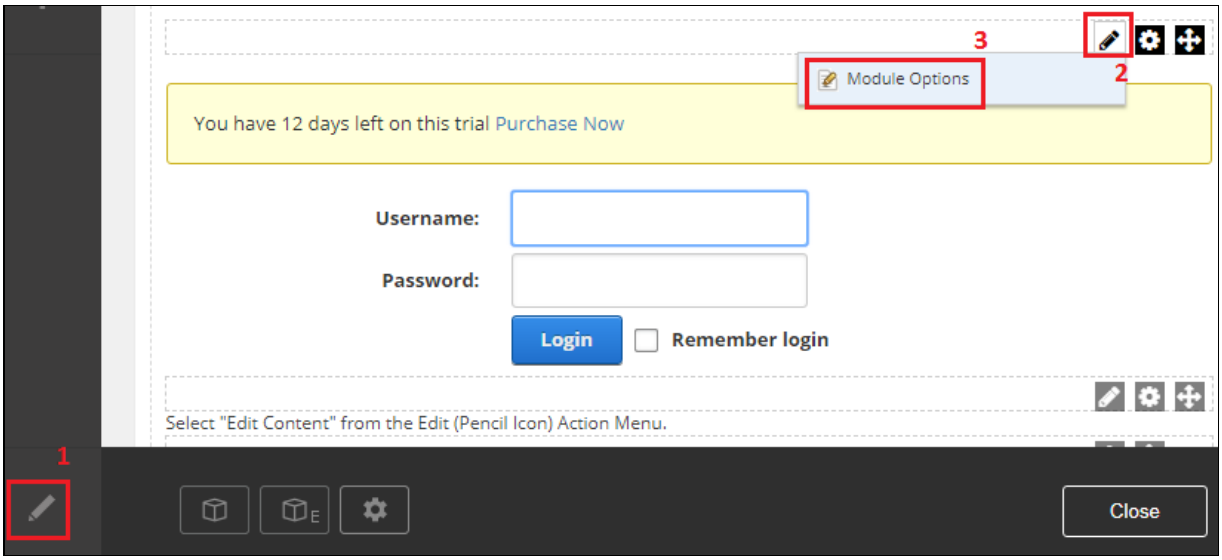
The ‘AD-Pro Authentication’ plugin allows you push Active Directory user profile to the DNN website. In other words DNN user can have the same profile properties as corresponding Active Directory user. You can determine what profile fields will be sync, you can even set custom profile mappings. Everything can be done through ‘Property manager’ tab.

> **Note:** Profile synchronization happens only at the user login process.

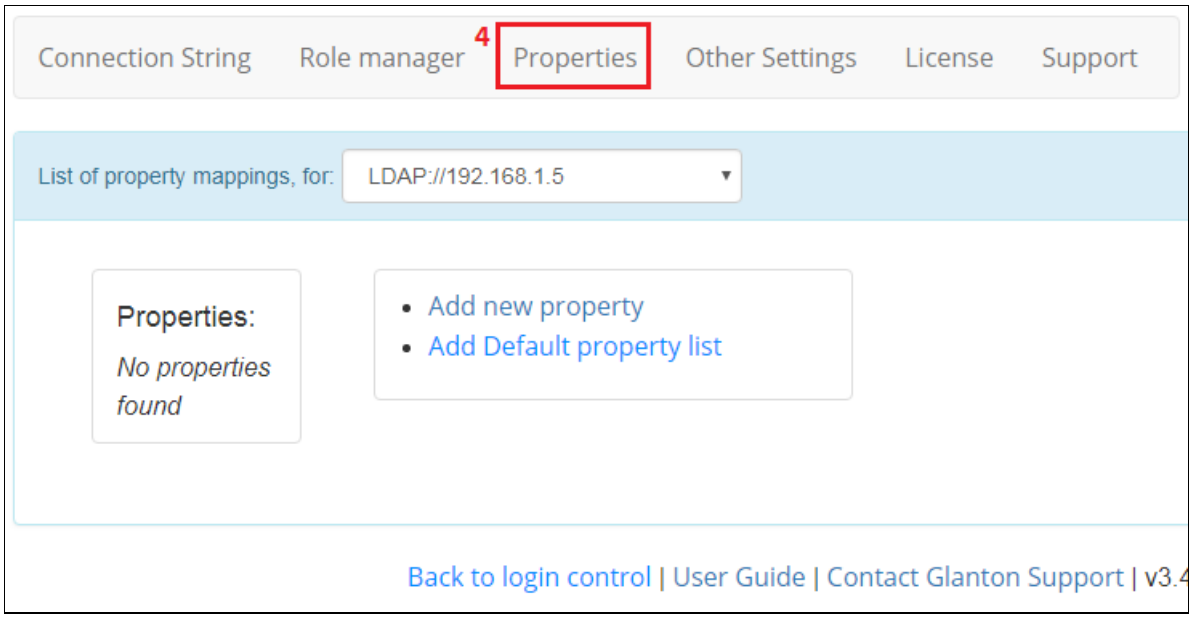
6.2. Setting up profile to sync

Below are the steps that needs to be done to set default list of properties that will be transfered from Active Directory to DNN. These properties are: First Name, Last Name, Middle Name, Street, Telephone, Cell, Fax, City, Postal Code and user avatar.

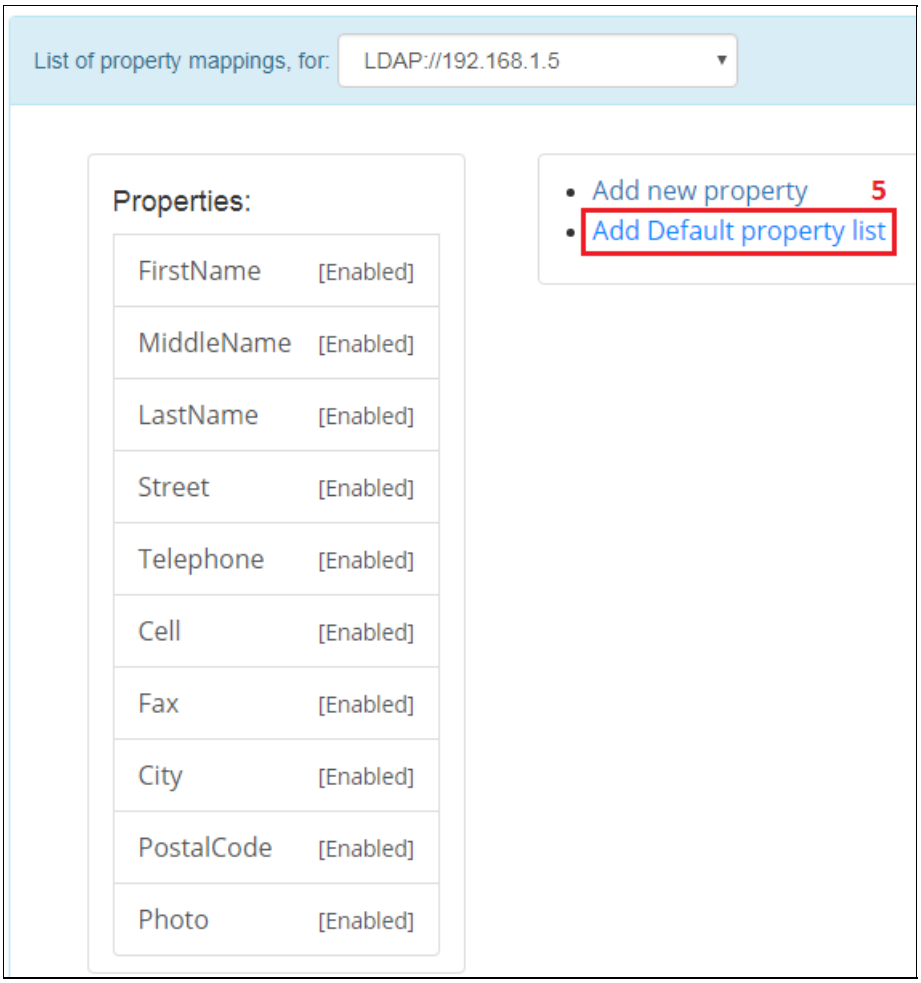
1. First sign in to DNN website as a ‘DNN Host’ or ‘DNN Administrator’.
2. Go to page where ‘AD-Pro Authentication’ module is placed.
3. Set DNN into ‘Edit’ mode, then go to ‘Module Options’, see figure below.



4. Go to 'Profile' tab, see image below.



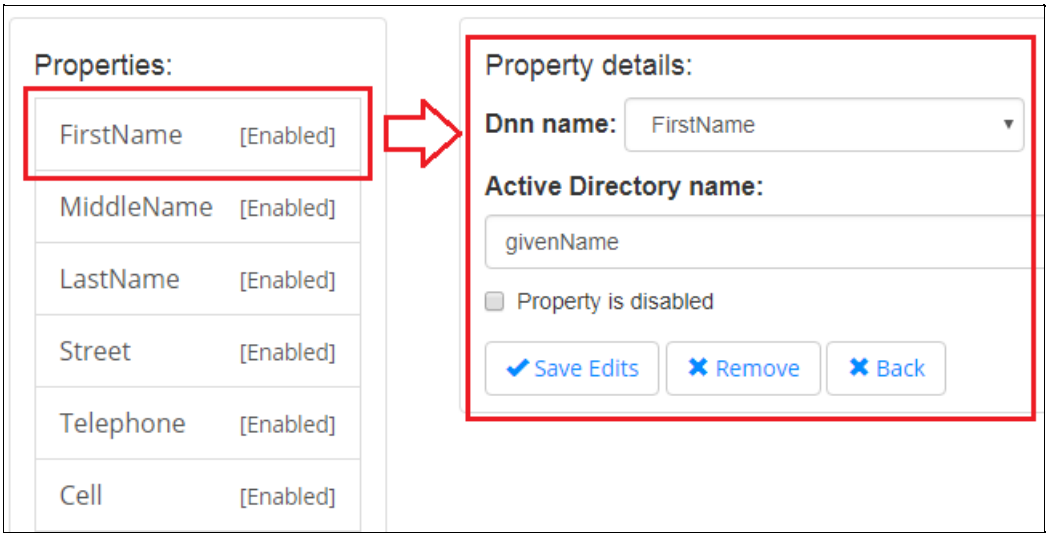
5. Click on `Add default property list` link. This will automatically add ten basic user profile fileds, see image below.



Now properties listed in the column will be transfered from AD to DNN user profile. Don't need to click any other 'save' button(s) to save that list in DNN.

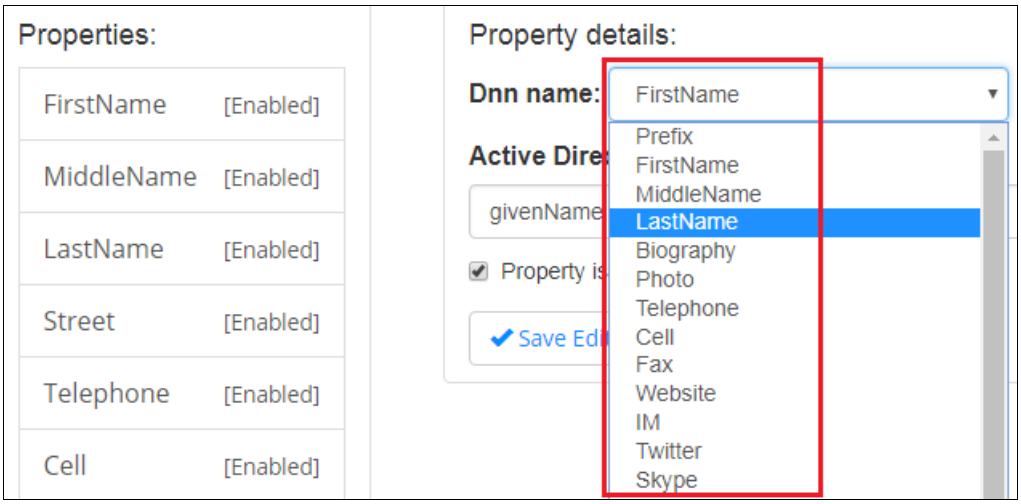
6.3. Customizing properties to sync

'Profile manager' allows you change details of properties to sync. You can do it by clicking on one of the profile property defined in the column. On the image below, are the details of the `First Name` property.



Particular profile property can be easily removed from the sync list, by disabling checkbox `Property is enabled`, then `Save Edits` button needs to be clicked.

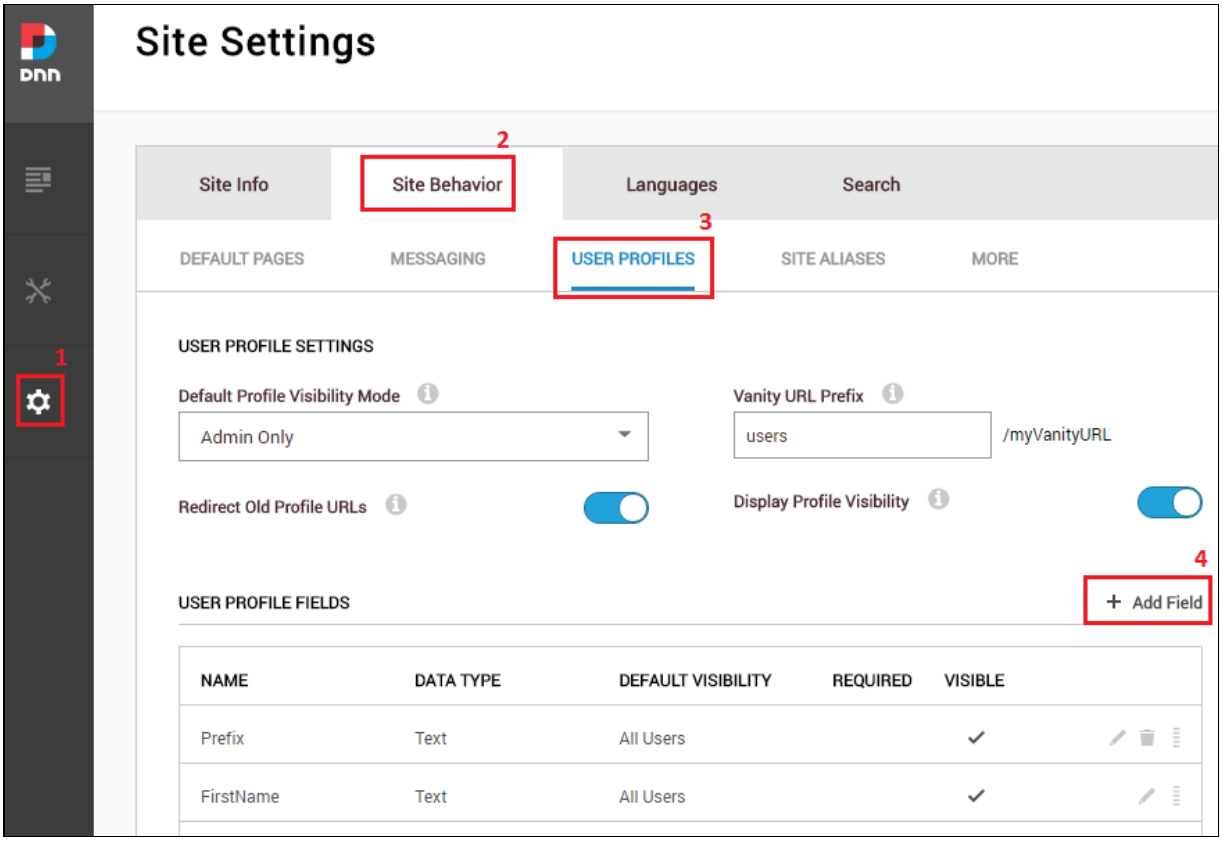
Target DNN property can be changed, be choosing other property from the `DNN name` drop down list, then `Save Edits` button needs to be clicked. See image below.



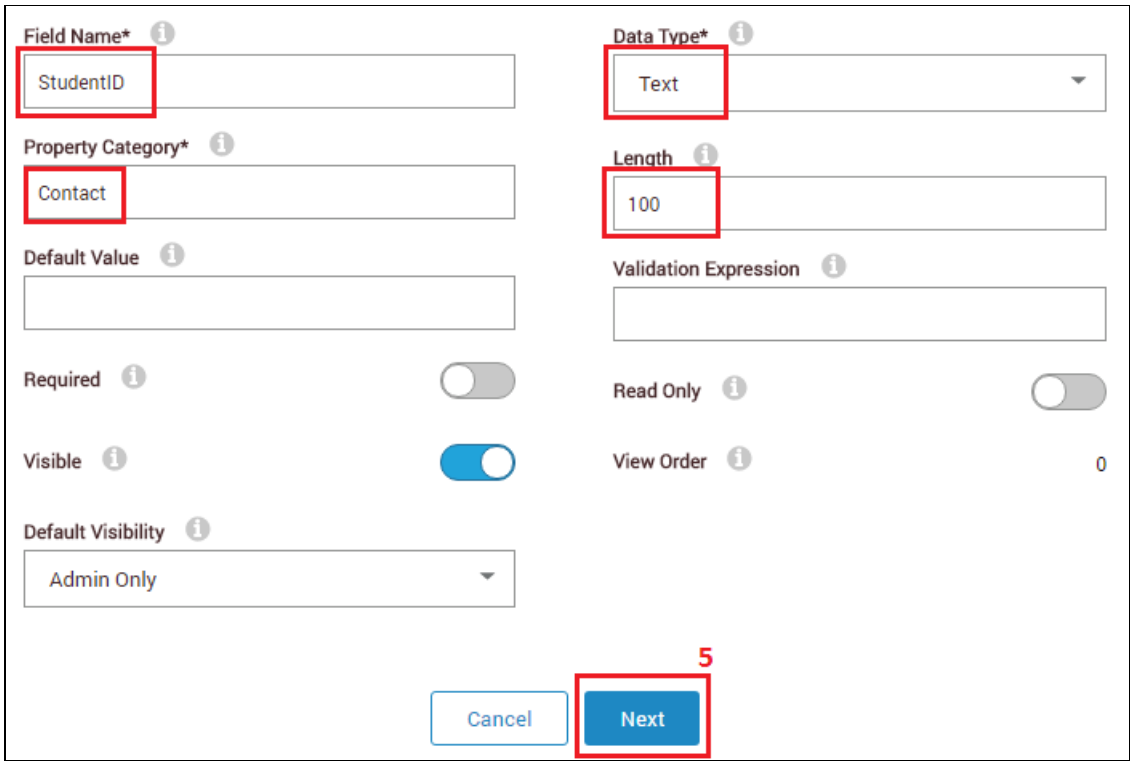
6.4. Custom property mapping

Active Directory users often have custom profile properties, something like a 'StudentID'. 'AD-Pro Authentication' module allows connect that custom AD property with DNN profile. We calle it 'Coustom Property Mapping'. Steps below will show how to set custom mapping between Active Directory user attribute 'StudentID' and DNN user profile field 'StudentID'.

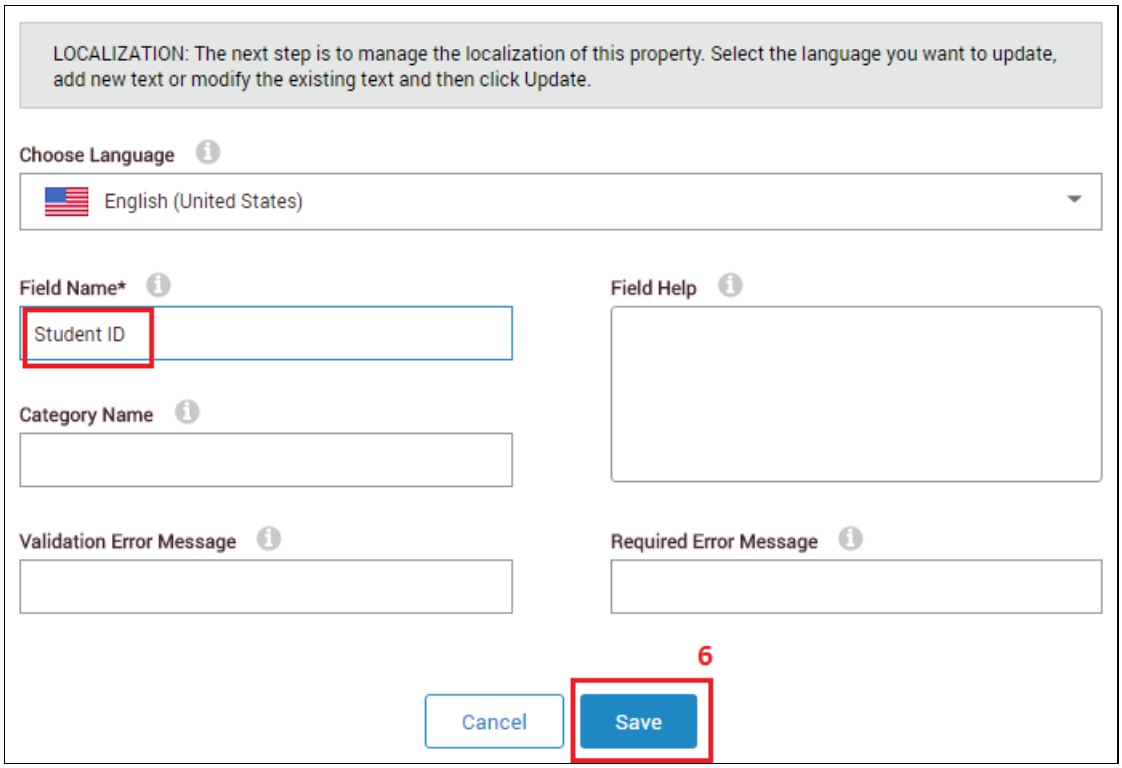
1. First create target DNN property `StudentID`. In this DNN property we will keep AD property. To do that go to 'Site Settings-> Site behavior-> User profiles' and click on `Add field` link, see image below.



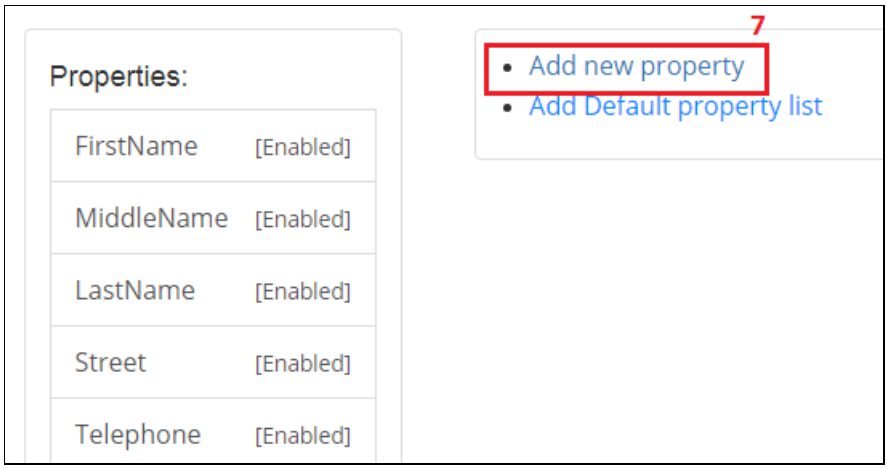
2. Fill the form, like on figure below and click 'Next' button.



3. Enter localized filed name, and click 'Save' button, see figure below.

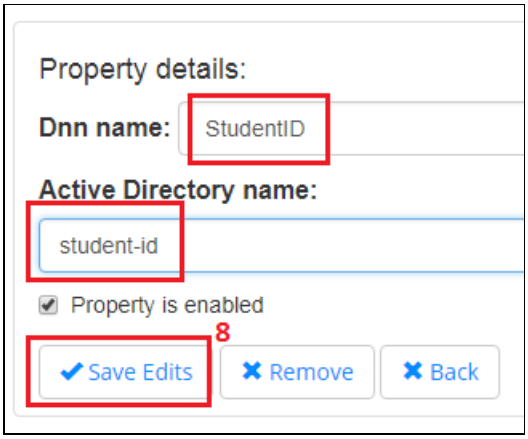


4. Back to 'AD-Pro Authentication' and 'Property manager', click on 'Add new property', see image below.

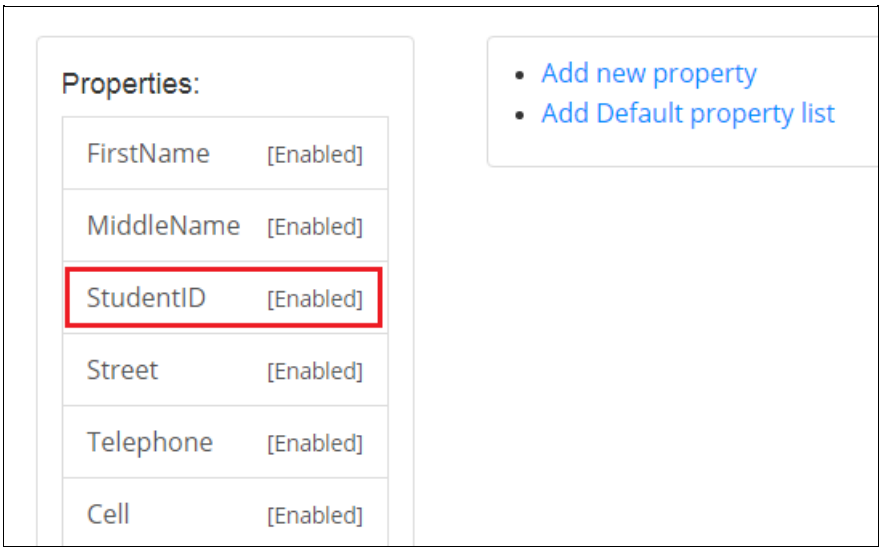


5. Inside the form enter DNN property name and coresponding Active Directory name, make sure that property is enabled then click on 'Save Edits' button, see figure below.

Note: Ask your Active Directory administrator for the exact attribute property name. In our case it's 'student-id'.



New property is added to the sync list, see image below. At the next sign up process, DNN 'StudentID' property will be populated.



7. Single Sign On

Note: Objective of this chapter is to show how to automatically sign in users to DNN website.

7.1. Overview

"AD-Pro Authentication v3" module have an option to login to DNN without entering any credentials, we call it Single Sign On (SSO). This scenario is possible only in intranet company networks. In addition, other conditions must be met and configuration steps can be tricky so please read whole chapter before you proceed. SSO is created at the top of the NTLM or Kerberos protocols, that are used in IIS

Windows authentication [1].

> **Note:** Before you start configuring SSO make sure that manual login is working properly.

7.2. Requirements

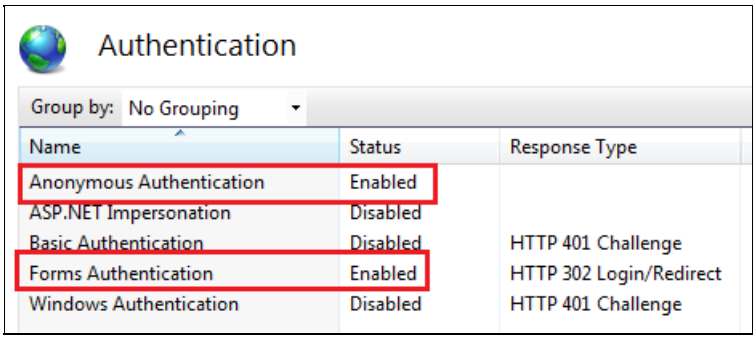
Following general conditions must be meet for SSO:

- IIS server where DNN website is located, must be part of the Active Directory system,
- before using SSO, user needs to be signed in to Active Directory,
- user who will use SSO must have correct file permissions to the folder where DNN website is located,
- web browser (IE/Firefox/Chrome) must be properly configured,
- finally the 'AD-Pro Authentication' plugin needs to be properly configured,

7.3. IIS Configuration

From the Internet Information Services (IIS) perspective following conditions must be met. First of all, DNN website needs to be hosted on IIS server, that is part of Active Directory domain. It's because between IIS and AD needs to be set up Kerberos [2] or NTLM protocol.

Furthermore, in IIS "Authentication" section for DNN website root folder, must be configured as described on figure below:

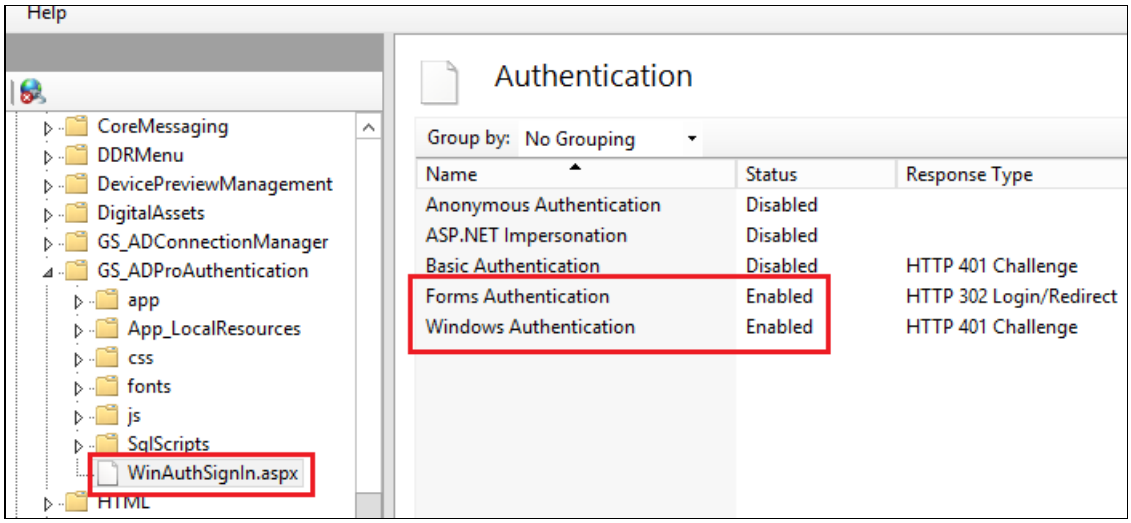


- Anonymous Authentication - Enabled,
- Forms Authentication - Enabled,
- Windows Authentication - Disabled,
- optionally ASP.NET Impersonation can be enabled,

Please note that on figure above 'Windows Authentication' is disabled, remember this is for the DNN website root. 'Windows Authentication' should be enabled for only one file: `~\DesktopModules\GS_ADProAuthentication\WinAuthSignIn.aspx` At the intalation process, 'AD-Pro Authentication' plugin automatically adds following code snippet to the `web.config` file, that enables 'Windows Authentication' for the `WinAuthSignIn.aspx` page:

```
<location path="DesktopModules/GS_ADProAuthentication/WinAuthSignIn.aspx">
    <!-- Disable Forms Authentication -->
    <formsAuthenticationWrapper enabled="false" />
    <system.webServer>
    <security>
        <!-- Enable IIS Windows authentication for the login page -->
        <authentication>
        <windowsAuthentication enabled="true" />
        <anonymousAuthentication enabled="false" />
        </authentication>
    </security>
    </system.webServer>
</location>
```

In result broker page `WinAuthSignIn.aspx` should be configured as on figure below.



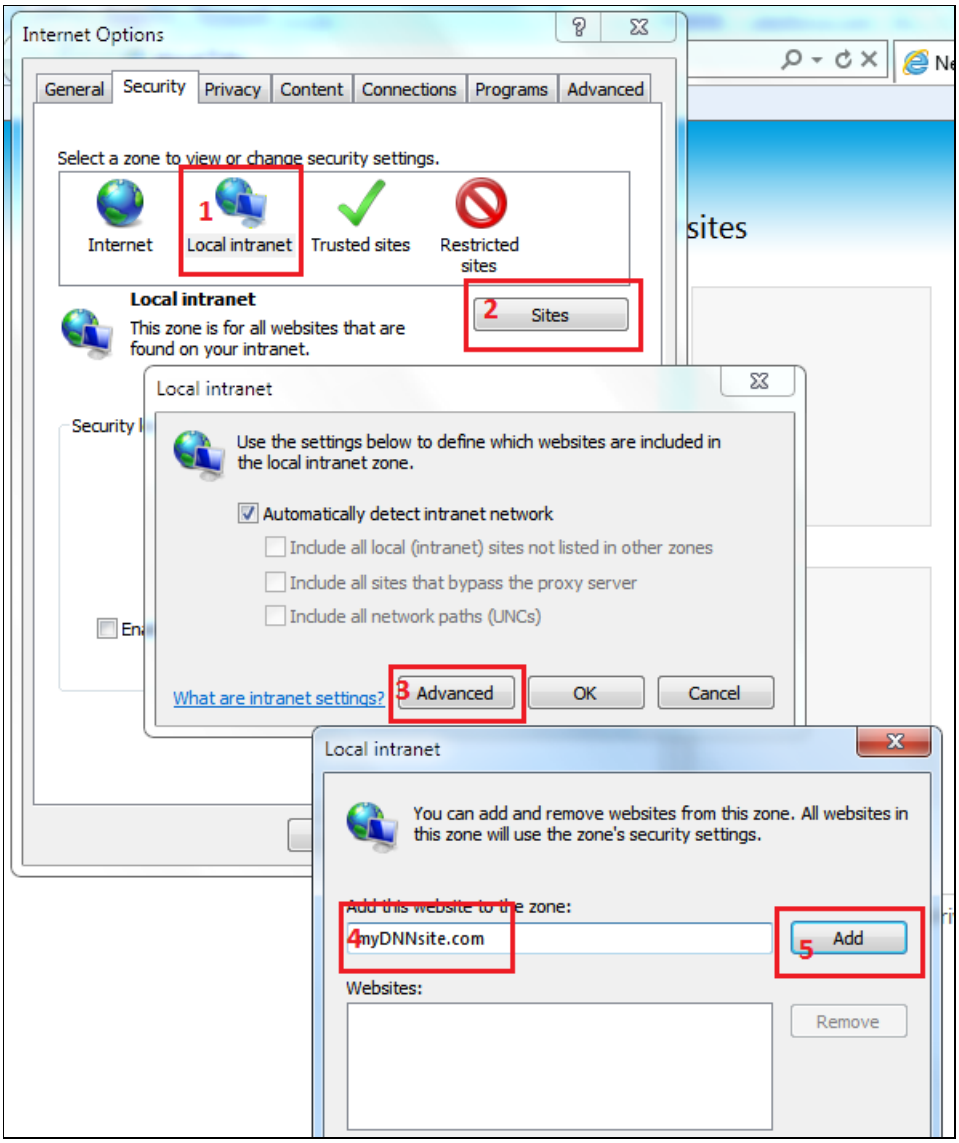
7.4. Web browser configuration

Web browser where DNN website is rendered, needs to expose user identity. Using this identity DNN is able to recognize user and SSO can happen. We strongly recommend configure Internet Explorer browser as a first one. If IE will work, you can focus on other browsers. We couldn't set up SSO with Safari.

7.4.1. Internet Explorer

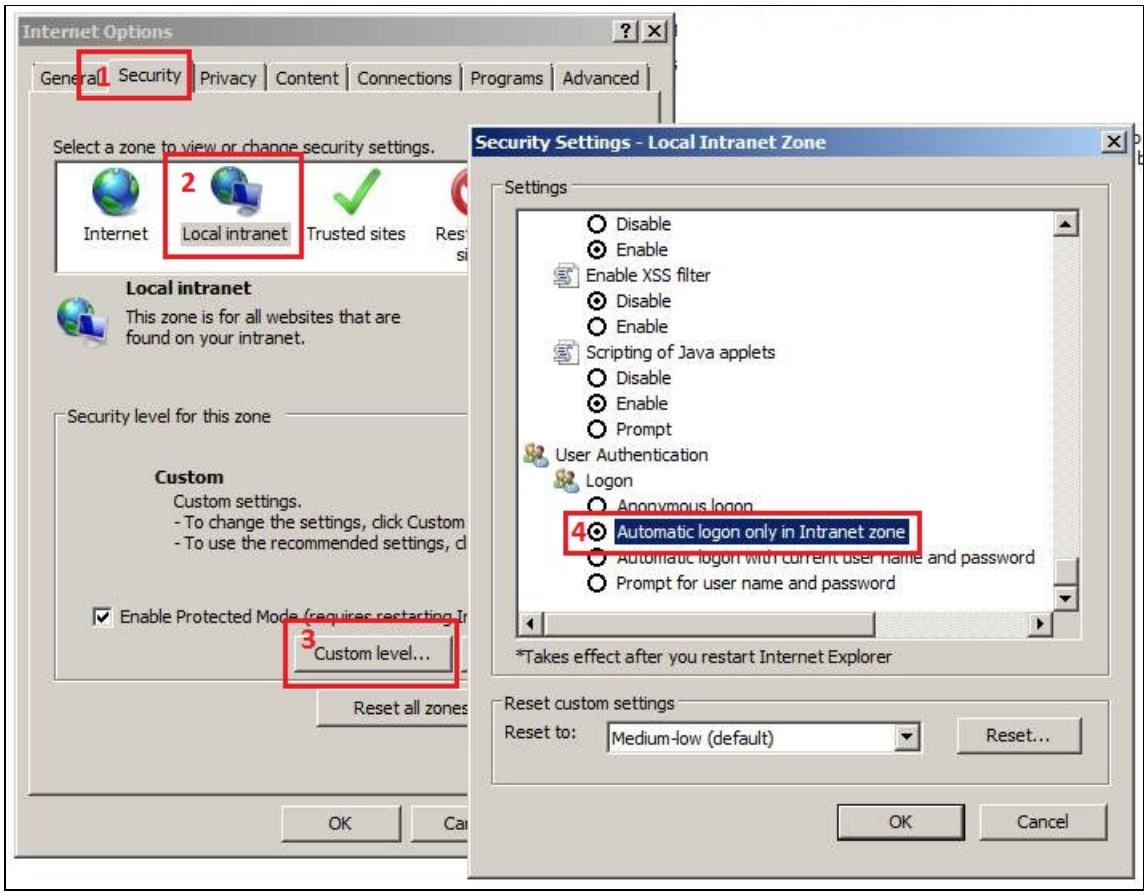
For the Internet Explorer execute following steps. First add DNN website to the**local intranet**.

1. Open Internet Explorer web browser.
2. Go to `Tools` -> `Internet options`.
3. Open `Security` tab.
4. Click on `Local Intranet` then `Sites` button.
5. Click on `Advanced` button (skip this step if popup will not be displayed).
6. List of intranet websites will be displayed, make sure that your DNN website is on it. If not, enter website name into `Add this website to the zone` text box and click `Add` button.
7. See figure below for more info.



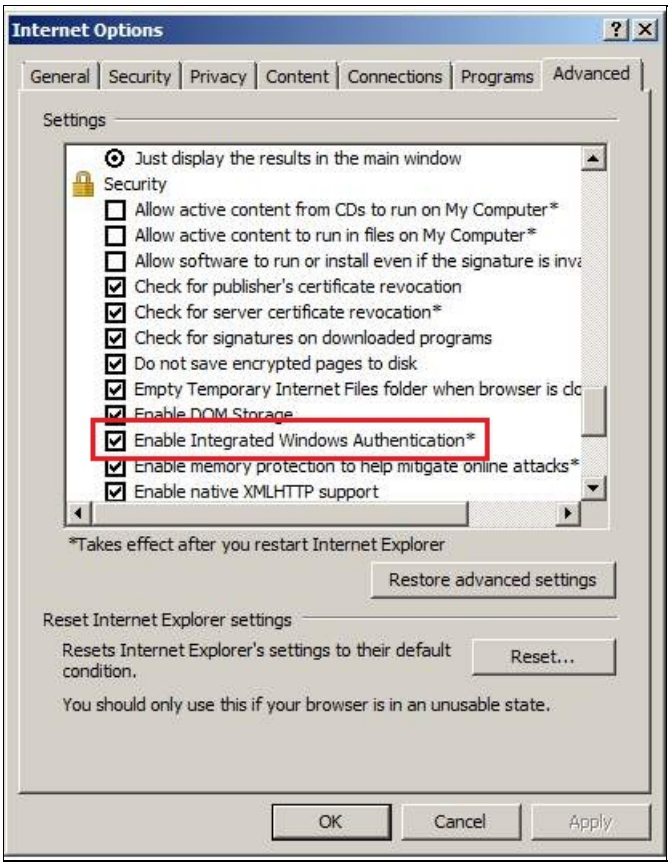
Second, enable **Automatic logon**:

1. Open Internet Explorer web browser.
2. Go to `Tools` -> `Internet options`.
3. Open `Security` tab.
4. Click on `Local Intranet` then `Custom level` button.
5. Inside `Security settings` enable `Automatic logon only in Intranet zone`.
6. Save settings.
7. See figure below for more info.



Thirdly, enable **Integrated Windows Authentication**

1. Open Internet Explorer web browser.
2. Go to `Tools` -> `Internet options`.
3. Open `Advanced` tab.
4. Make sure that `Enable Integrated Windows Authentication` is enabled (ticked). This option takes effect after you restart Internet Explorer.
5. See figure below for more info.



7.4.2. Chrome

Chrome uses the same intranet settings as Internet Explorer, so if it's working in IE it will also work in Chrome (without any additional settings).

7.4.3. FireFox

To configure Firefox browser follow steps below:

1. Put string `about:config` in url address field and press enter.
2. In filter box type `network.automatic-ntlm-auth.trusted-uris`
3. Modify `network.automatic-ntlm-auth.trusted-uris`, add url of your DNN domain or IP address.
4. To specify all subdomains use `.replacewithyoursite.com` instead of: `www.replacewithyoursite.com`, `help.replacewithyoursite.com`, `pictures.replacewithyoursite.com`

7.5. Auto SSO

By default user first needs to go to DNN login page to initiate SSO process. You can make that process even simpler. The point is to permit access for "Guest" users, what will result transparent auto SSO.

If all DNN pages will have permissions `View` for `Registered Users` (page will be blocked for `Guest` user). User will be automatically redirected to the DNN login page, where SSO process will be executed. This scenarrio initiates transparent login process, where users are allways automatically signed in to DNN website.

7.6. Skip SSO

If you want to skip auto SSO, for example to sign in as DNN "host" or "admin", a special query string parameter needs to be added to the login page: `sso=false`.

The url address can look as follow: `www.MyDnn.com\login.aspx?sso=false`

7.7. SPN & Kerberos

To use SSO which is in fact Kerberos authentication, the following conditions must be met. Usually default AD configuration is OK, but if for some reason SSO will fail, it's good to get familiar with this chapter.

- the client and server computers must be part of the same Windows domain, or in trusted domains,

- Service Principal Name (SPN) [3] must be registered [4] with Active Directory, which assumes the role of the Key Distribution Center in a Windows domain. The SPN, after it is registered, maps to the Windows account that started the Internet Information Server (IIS) instance service. If the SPN registration has not been performed or fails, the Windows security layer cannot determine the account associated with the SPN, and Kerberos authentication will not be used,

- to use Kerberos [2] authentication, a service must register its service principal name (SPN) [3] under the account in the Active Directory directory service that the service is running under. The service principal name (SPN) is a multivalued attribute. It is usually built from the DNS name of the host. The SPN is used in the process of mutual authentication between the client and the server hosting a particular service. The client finds a computer account based on the SPN of the service to which it is trying to connect. The SPN can be modified by members of the Domain Admins group. By default, Active Directory registers the network basic input/output system (NetBIOS) computer name. Active Directory also permits the Network Service or the Local System account to use Kerberos,

- SPN is nothing more fancy than an alias (or pointer) for a domain account. Let's say that ther is a Windows Server 2012 server called `WebServ` (with IIS) that is member of the Active Directory domain `cloudapp.net`. On the web server you have DNN application that is using url ⇗http://webserv.cloudapp.com below is output of a `setspn -l` command [4]:

```
HOST/WEBSERV
HOST/webserv.cloudapp.net
```

7.8. SSO Troubleshooting

Here is a list of common issues that you can meet configuring SSO for Active Directory. Before you contact Glanton Support, take a look at our guide to the most common SSO problems that could be fixed.

7.8.1. Hosts file

By default SSO will **not work** for sites that are specified in: `C:\Windows\System32\drivers\etc\hosts` file. IE will not auto log you into the site, nor will you be able to login by providing the correct credentials. The reason for this is that in Windows Server 2003 SP1 a new security functionality called "loopback check" was added, this blocks the authentication request and so for your site to work with the new-host name locally you need to disable the loopback check. Below is an example how to disable loopback check functionality for `CNAME = dnn920.com` follow steps:

1. Click `Start`, click `Run`, type `regedit`, and then click `OK`.
2. Locate and then click the following registry subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0`
3. Right-click `MSV1_0`, point to `New`, and then click `Multi-String Value`.
4. In the Name column, type `BackConnectionHostNames`, and then press `ENTER` key.
5. Right-click `BackConnectionHostNames`, and then click `Modify`.
6. In the `Value` data box, type the `dnn920.com`.

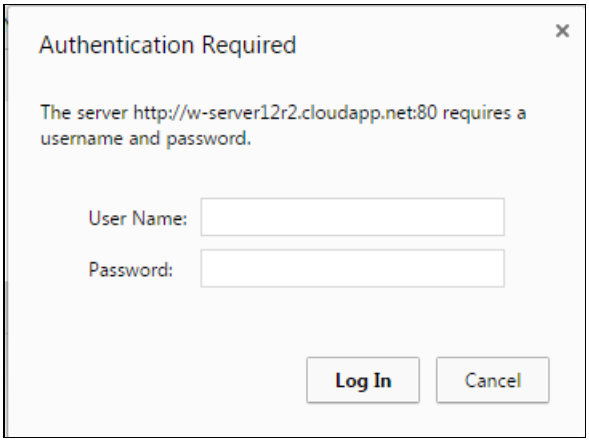
7. Exit Registry Editor, and then restart the computer.

8. Type each host name on a separate line. If the `BackConnectionHostNames` registry entry exists as a `REG_DWORD` type, you have to delete the `BackConnectionHostNames` registry entry.

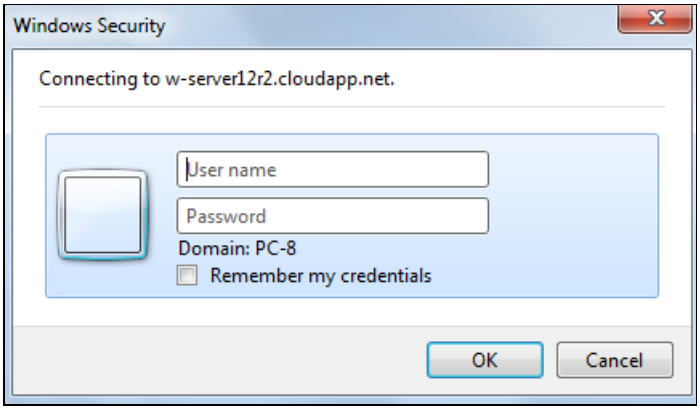
More info can be found ⇗in this post

7.8.2. Error screen for external users

When SSO is enabled all users can transparently sign in from inside the company, but extrnal users encounter inconvenience. If somebody want to see website from outside company, an web browser will display security login popup, like on the screen below:

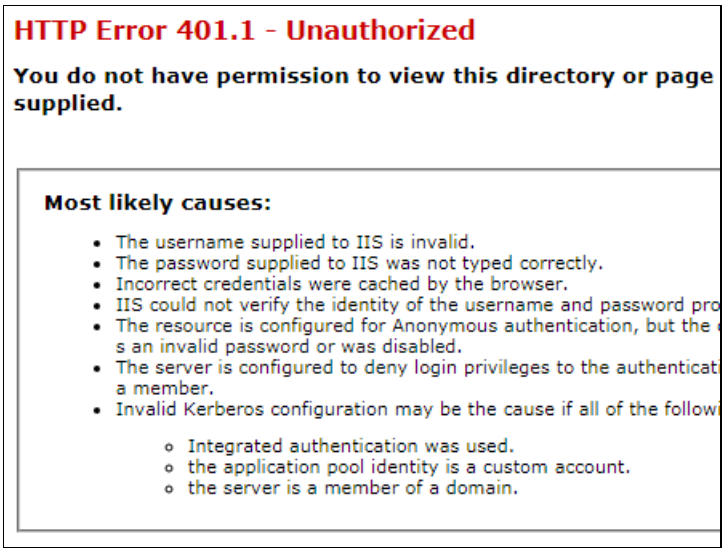


Chrome popup version



Internet Explorer popup version

And if user will click `Esc` or `Cancel` to skip that popup, another ugly error will appears, see image below:



As a workaround we suggest configure costom login page for `401 HTTP` erros. To do that follow seteps below:

1. Copy file from `~\DesktopModules\GS_ADProAuthentication\401.htm` to the DNN `bin` directory.

2. Add to the `web.config` file, under section `<system.webServer>`, folowing entry:

```
<httpErrors errorMode="Custom">
    <remove statusCode="401" />
    <error statusCode="401" path="401.htm" responseMode="File" />
</httpErrors>
```

Now security popup will still appears, but when user click `Esc` or `Cancel` button, he will be redirected to the login page. Security login popup issue is a result of Kerberos protocol, and for now we don't know how to get around it.

7.8.3. Login screen after user inactivity

In SSO mode, users can get login popup after certain period of inactivity. Usually it's because cookie expiration, that can be easily extended to 5 days (7200 min.):

1. Open the `web.config` file.

2. Go to section `<configuration> -> <appSettings>`,

3. For key `PersistentCookieTimeout` set value `7200`, example: `<add key="PersistentCookieTimeout" value="7200" />`

7.8.4. Kerberos fails

SSO works at the top of the Kerberos protocol, please get familiar with ⇗this article that could help diagnose Kerberos issues.

References

[1] Microsoft doc explaining ⇗IIS and Windows Authentication

[2] *(1, 2)* Microsoft doc explaining ⇗Kerberos protocol

[3] *(1, 2)* More info about ⇗SPN

[4] *(1, 2)* ⇗Registering SPN

[5] Things to check when ⇗Kerberos fails

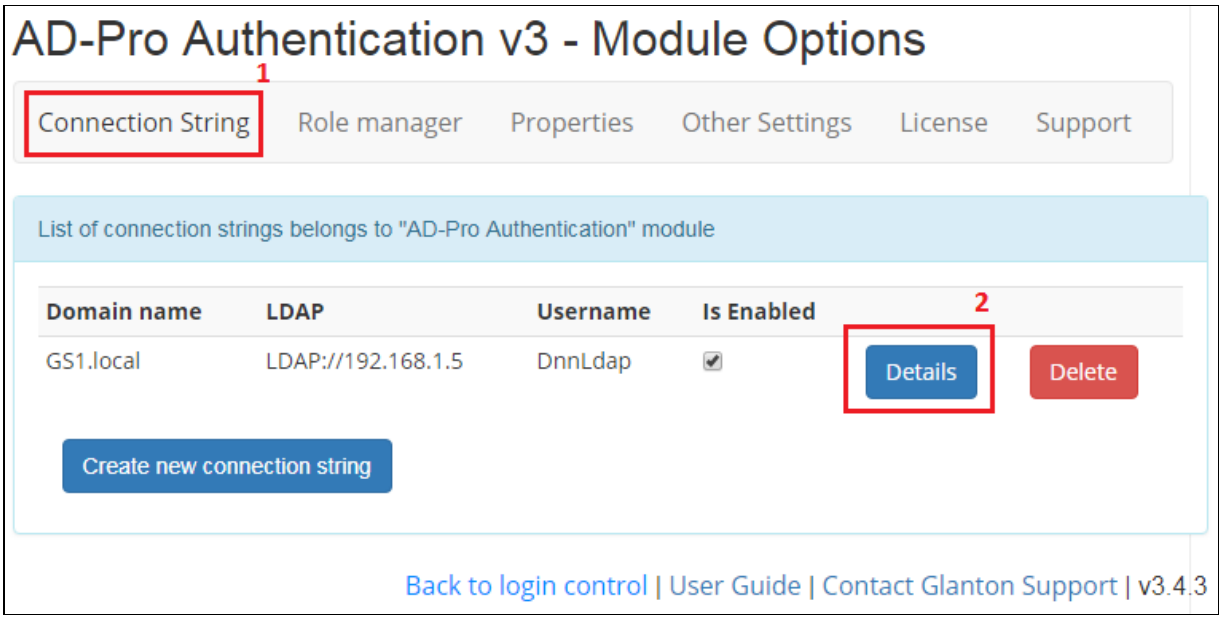
8. Advanced Settings

> **Note:** In this chapter we described more advanced features of "AD-Pro Authentication" module. It's not necessary to read this in order to configure simple login scenario, but if your users already can sign in, here you can find info how to adjust or optimize that process.

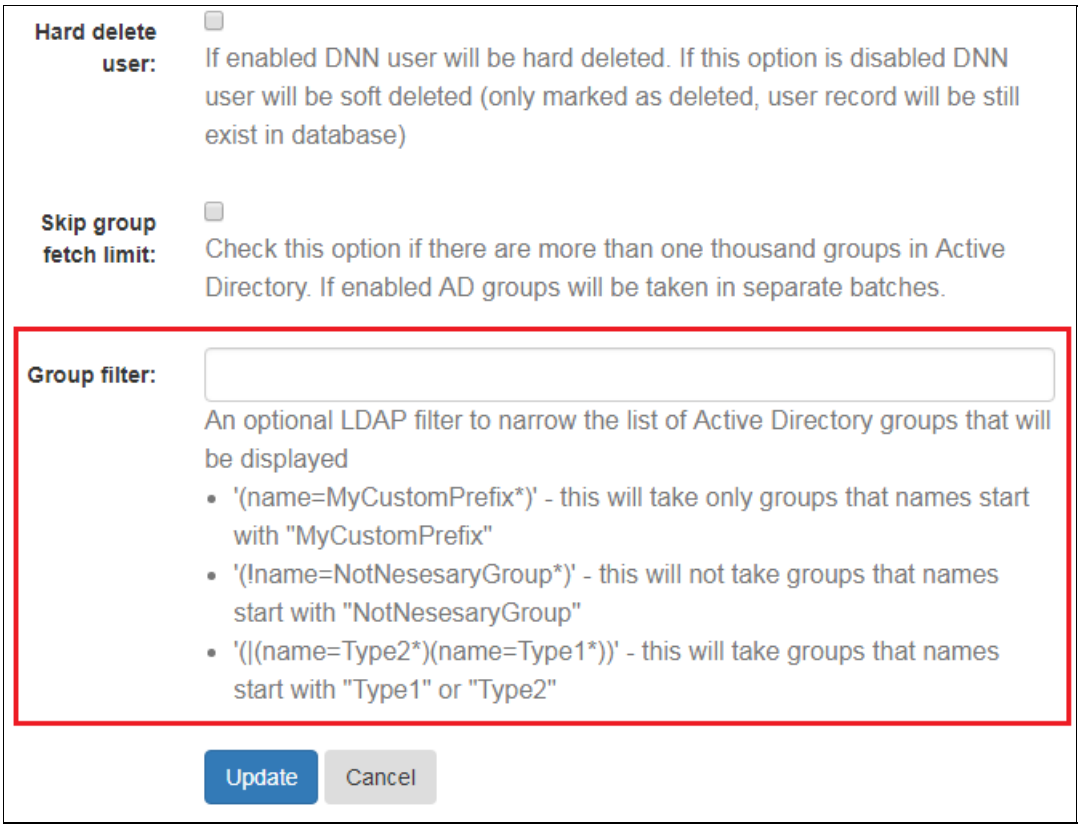
8.1. Group filter

If your Active Directory system contains lot's of groups, it's good to narrow that list. Fewer AD groups are easier to manage and speed up login process, because DNN doesn't need to iterate through all of them. This setting has impact in 'Role Manager' tab, where only groups that pass this filter will be displayed. To add or edit "Group Filter" setting, follow these steps:

1. Click on "Connection String" tab, then on "Details" button, see figure below.



2. At the end of this form is a text box where group filter can be entered, see figure below.



Below are some filter examples:

1. `(name=MyGroupPrefix*)` will takes only groups that starts with `MyGroupPrefix`.
2. `(!name=NotNecessaryGroups*)` will takes all AD groups except groups that names starts with `NotNecessaryGroups`.
3. `(|(name=Domain*)(name=Alpha*))` will takes all AD groups that names starts with `Domain` or `Alpha`.
4. Empty text box, means no grup filter, in this case all groups will be taken.

8.2. LDAP filters

Note: LDAP syntax filters are used to query Active Directory users or groups.

A filter specifies the conditions that must be met for a record to be included in the recordset (or collection) that results from a query. To implement `AND` operator please use `&`. This snippet will take groups that names start with 'T' and ends on 'Z':

```
(&(name=T*)(name=*Z))
```

To implement `OR` operator please use `|`. This snippet will take groups that names start with 'Type1' or 'Type2':

```
(|(name=Type2*)(name=Type1*))
```

More info: https://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx

8.3. Authentication ticket management

Authentication ticket is used to tell ASP.NET application who you are. The "AD-Pro Authentication" saves authentication ticket in the cookie. There are two kinds of cookies:

- session cookie, that is saved in the browser session and deleted when user close the browser. When the browser is restarted the DNN website will not recognize you because cookie and authentication ticket (that is inside it) doesn't exist. User will have to log back in (if login is required). After that, a new session cookie will be created (with new authentication ticket inside it) and will be active until user leave the site or close the browser;

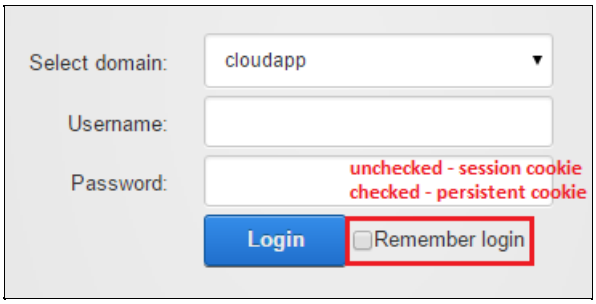
- persistent cookie, it's a file that is saved on the user hard disk. It can be deleted manually or browser deletes it based on the duration period contained in the persistent cookie's file. In that mode user can be signed-in across browser sessions, after browser is reopened, even after one day of inactivity.

Cookie names that are created by "AD-Pro Authentication" are:

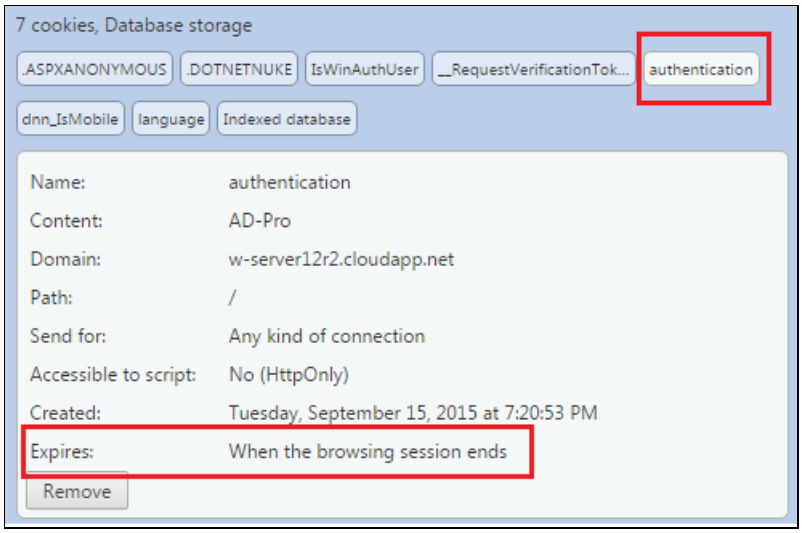
- `IsWinAuthUser`, if value is `True` currently sign-in user is a SSO user, if value is `False` currently logged in user was sign-in manually; if cookie doesn't exist or cookie value is empty, user is not signed-in (or signed-in incorrectly);

- `authentication`, the cookie value can be equal to string `AD-Pro`. If cookie doesn't exist or cookie value is empty, user is not signed-in (or signed-in incorrectly);

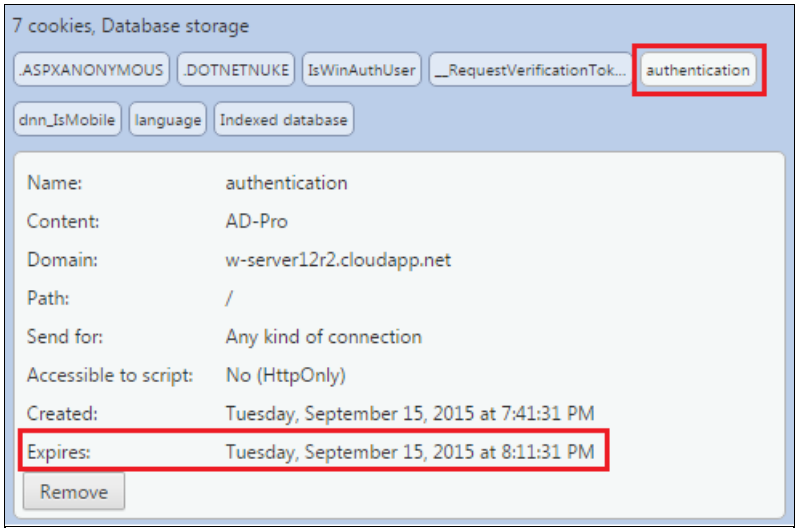
The "AD-Pro Authentication" creates session cookies when a user took advantage of SSO or when a user was signed-in manually and "Remember me" was unchecked.



Below is example of the session cookie:



The "AD-Pro Authentication" creates persistent cookies when user was signed-in manually and `Remember me` was checked. In that case cookie can look like this:

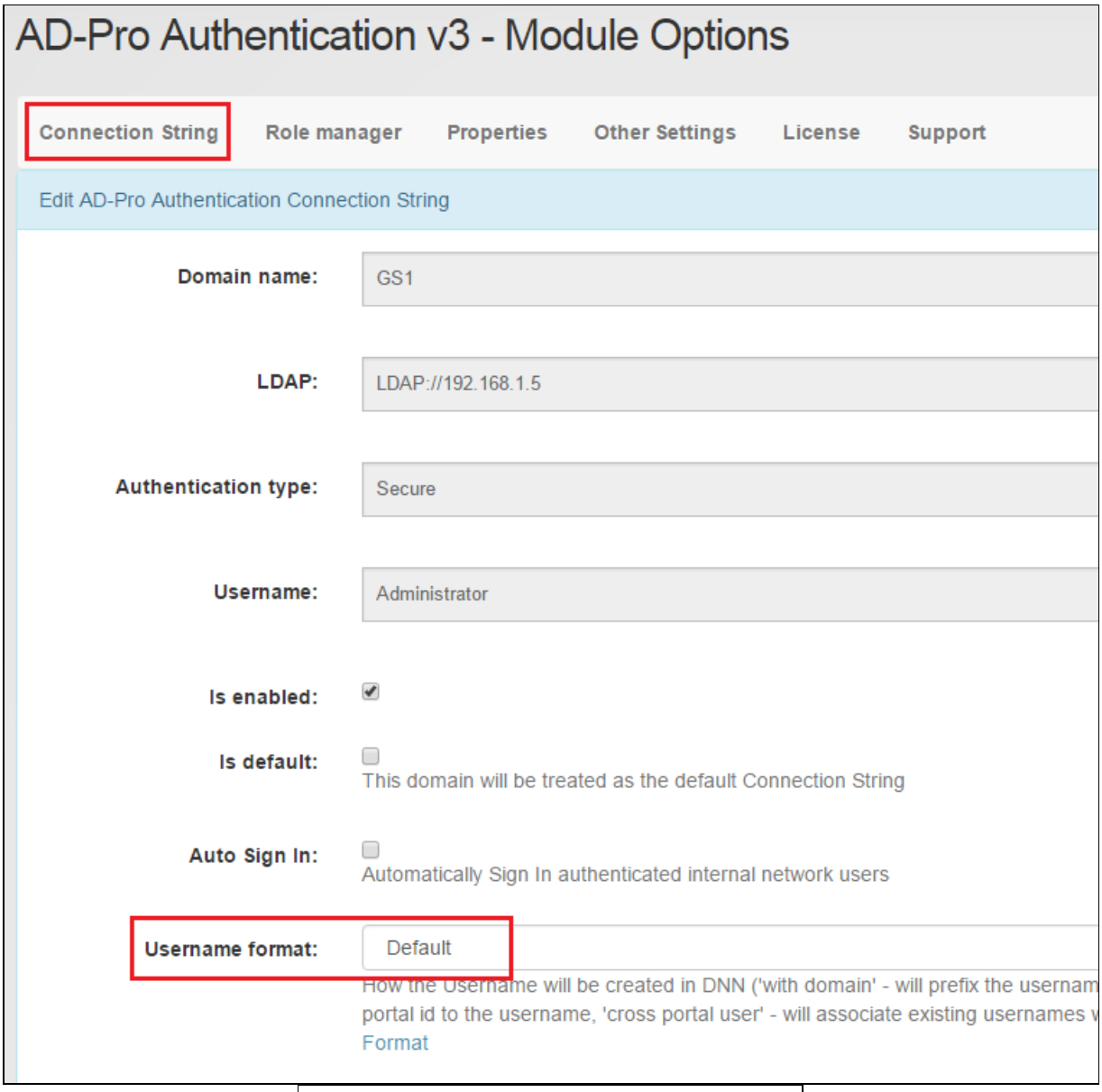


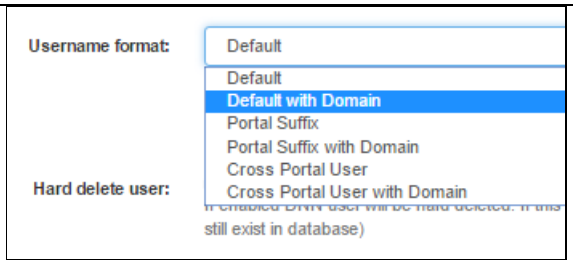
If `Remember me` mode is enabled, there is possibility to control the time when the user session will expire. On the figure above user will be signed-off after 30 min of inactivity. The expiration time can be controlled from the `web.config` file. The module first checks the `PersistentCookieTimeout` variable, if it's empty or equal to `0`, number of minutes will be taken from variable `timeout` that is in `configuration/location/system.web/authentication/forms` or, if it's also empty, from `configuration/system.web/authentication/forms`. If all variables will be also equal to `0`, timeout will be set to 30 min.

8.4. Username formats

> **Note:** It's very important to get familiar with this section, if you are using more that one DNN portal, or more than one Active Directory domain.

The "AD-Pro Authentication" module allows store DNN users in multiple modes. This options can allow to save one AD user in multiple DNN portals, where he can have separate profile. Please remember that in DNN database, in table `Users`, column `username` needs to be unique. Username format feature can be specified in "Module Options-> Connection String-> Details". See figures below.





Possible formats how the DNN username can be saved in database. Example for AD user called `Barry`, AD domain `GS`, and DNN portal id `2`

Username Format	Output example
Default	Username -> `Barry` Active Directory user can exit only in one (specified) DNN portal (in one portal across DNN install). In this situation AD user Barry is able to login to only one DNN portal (portal id = 2).
Default with Domain	AdDomain\Username -> `GS\Barry` Active Directory user can exit only in one (specified) DNN portal (in one portal across DNN install). In this situation AD user Barry is able to login to only one DNN portal (portal id = 2).
Portal Suffix	Username_{Portal ID} -> `Barry_2` Active Directory user Barry can exist in each portal and it will be separate user instance. In fact every DNN portal contains his own DNN user, that points to one Active Directory user.
Portal Suffix with Domain	AdDomainUsername_{Portal ID} -> `GS\Barry_2` Active Directory user Barry can exist in each portal and it will be separate user instance. In fact every DNN portal contains his own DNN user, that points to one Active Directory user.

Username Format	Output example
Cross Portal User	Username -> `Barry` Active Directory user can exist in each DNN portal, his username will be the same, with independent user profile. AD user Barry is able to login to any DNN portal. To enable this mode all "AD-Pro Authentication" instances across DNN install, should have "Username format" set to "Cross portal User". More info about the "Multi User" feature that allows to re-use username, can be found at this location: ⇗http://www.dnnsoftware.com/wiki/page/Users-in-multiple-portals-in-a-single-DNN-Instance
Cross Portal User with Domain	AdDomainUsername -> `GS\Barry` Active Directory user can exist in each DNN portal, his username will be the same, with independent user profile. AD user Barry is able to login to any DNN portal.

By default "Multi User" mode is working only for newly created DNN users (it's a DNN limitation), that's because members must have the same password across all DNN portals. This condition is not fulfilled for already existing users that already have "some" password. To enable "Multi User" feature for already created users please execute following SQL query, that will reset password for group of users:

```
UPDATE aspnet_Membership SET
Password = {New Password},
PasswordSalt = {New Password Salt}
WHERE UserId =  {list of the users to update}
```

9. Migration from DNN.ActiveDirectory provider

9.1. Overview

"DNN.ActiveDirectory" provider is a open source plugin created in 2012 by Mike Horton. Install package as well as the source code is available in ⇗Git repository

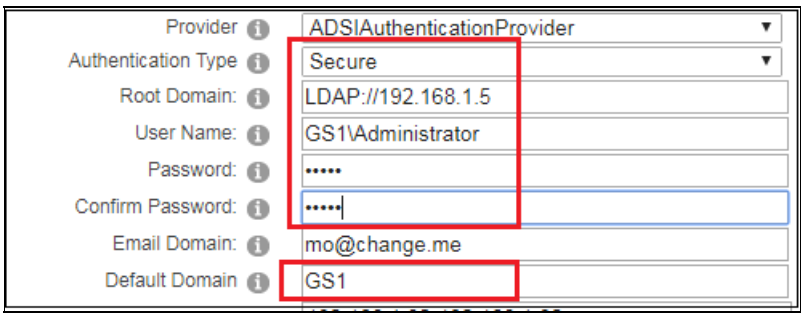
Move to "AD-Pro Authentication" plugin will mean fewer compatibility issues in DNN v8/9/Evoq. When you do decide to move forward, Glanton recommends you migration steps below.

9.2. Settings worth to note

"DNN.ActiveDirectory" settings can be reused. Before you uninstall "DNN.ActiveDirectory" provider copy following settings because "AD-Pro Authentication" will need it:

- Default Domain
- Root Domain also known as LDAP
- Username
- Password, it's encrypted
- Authentication type

See figure below:



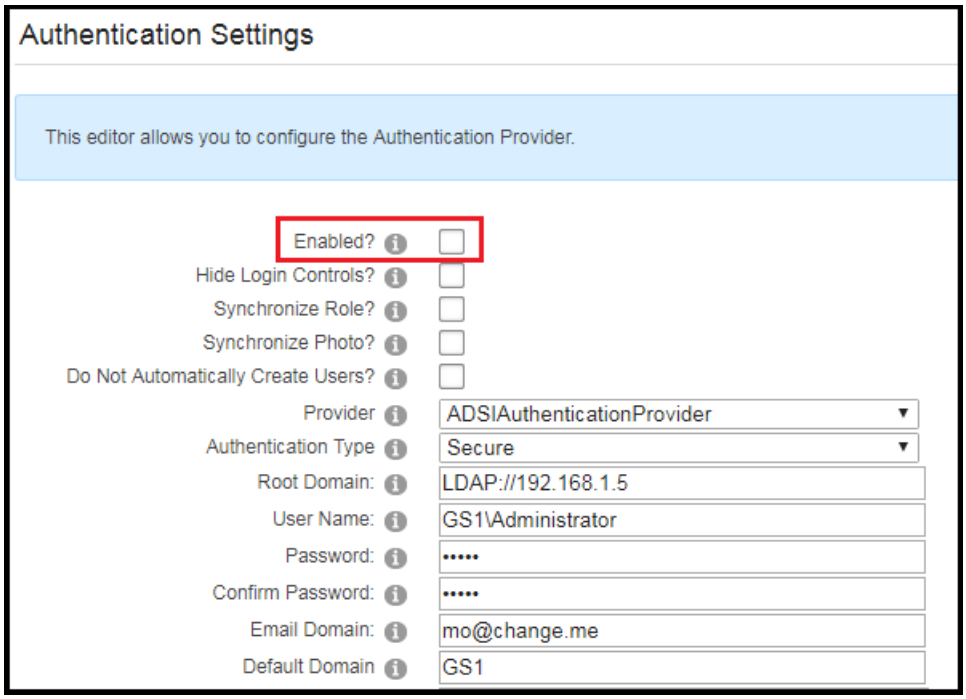
In case the provider menu is not available, same settings can be found in DNN database. Execute following SQL query to display "DNN Active Directory" config:

```
SELECT * FROM PortalSettings WHERE SettingName LIKE 'AD_%'
```

9.3. Disable “DNN.ActiveDirectory”

Before you install AD-Pro plugin, the “DNN Active Directory” needs to be disabled to prevent any conflicts.

1. In Authentication Settings set plugin into `Disable` mode.



2. In `web.config` file comment following lines:

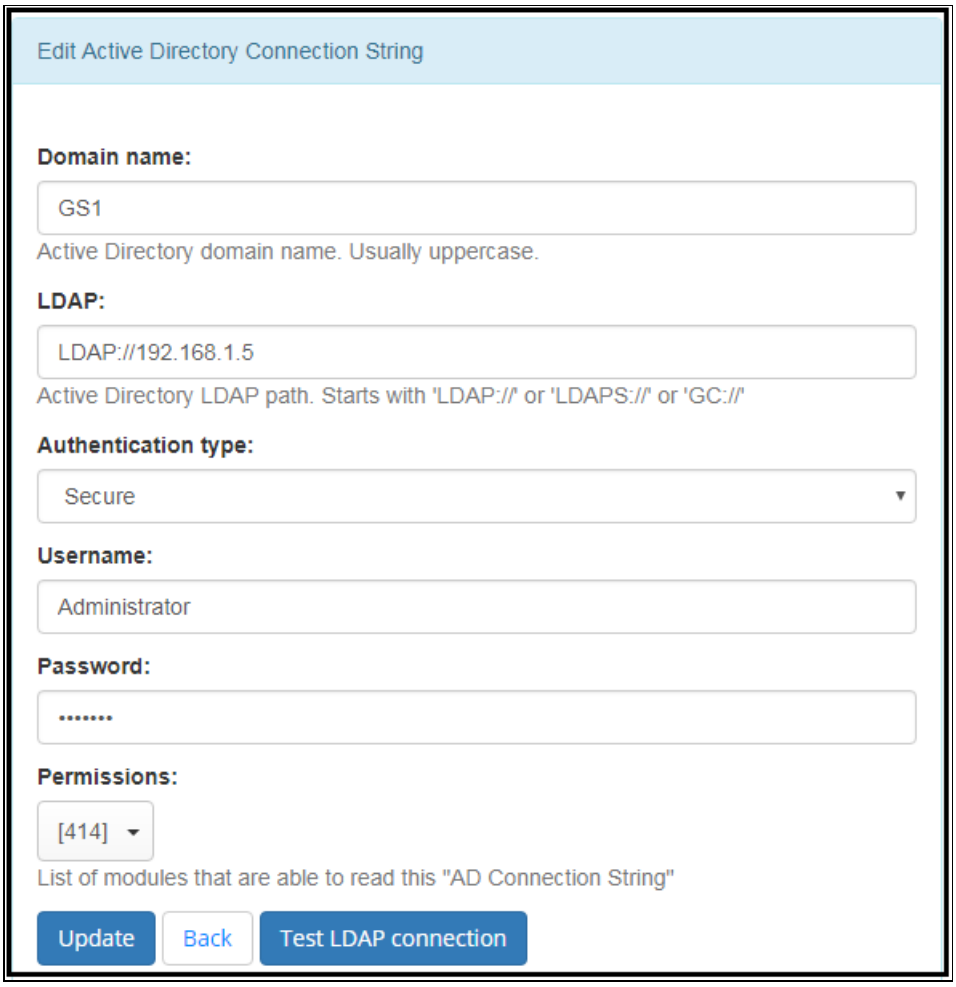
```
<location path="DesktopModules/AuthenticationServices/ActiveDirectory/WindowsSignin.aspx">
<!-- Disable Forms Authentication -->
    <formsAuthenticationWrapper enabled="false" />
    <system.webServer>
        <security>
            <!-- Enable IIS Windows authentication for the login page -->
            <authentication>
                <windowsAuthentication enabled="true" useKernelMode="false">
                    <providers>
                        <clear/>
                        <add value="NTLM"/>
                    </providers>
                </windowsAuthentication>
                            <anonymousAuthentication enabled="false" />
            </authentication>
        </security>
    </system.webServer>
</location>
```

9.4. Install “Connection Manager” & “AD-Pro Authentication” module

Now you are ready to install “Connection Manager” & “AD-Pro Authentication” module. This process is welly described in separate sections:

- ⇗Connection Manager installation process
- ⇗AD-Pro Authentication installation process

“DNN.ActiveDirectory” usually saves DNN usernames in format `Domain\Username`. To keep consistency, set in “AD-Pro Authentication” username format to Default with domain, here is more info about available username formats. Same username format allows reuse DNN identities created by “DNN.ActiveDirectory” provider. Same settings imported to “AD-Pro” plugin will look as on figure below:



9.5. Summary

If you will have any troubles, Glanton will support your journey to “AD-Pro Authentication”.

10. Troubleshooting

10.1. Diagnostic Mode

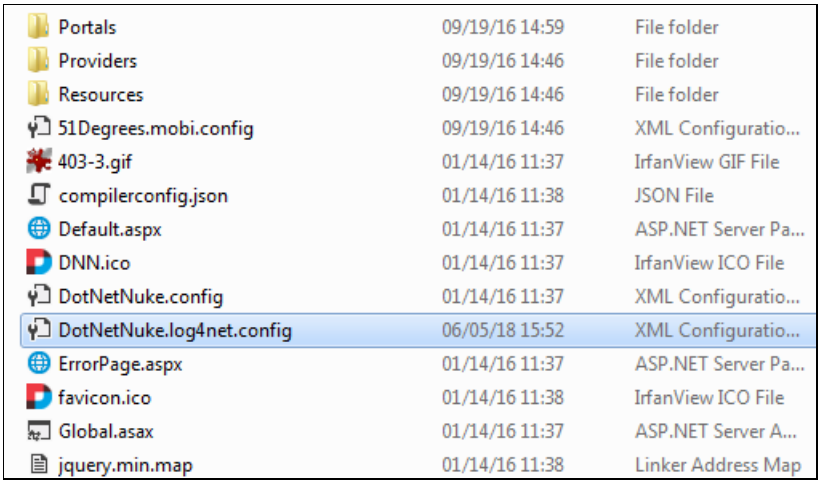
> **Note:** Diagnostic Mode will collect additional information that will help troubleshoot the issues.

If module doesn’t work as you expect, it’s worth to enable “Diagnostic Mode”. This will output logs that describes how the module is working. They can also diagnose issues that can occur like: config errors, failed login process, etc. Logs are created in file that is located in `~\Portals\_default\LogsYYYY.MM.DD.logs.resources`, see log example below:

```
[Thread:11][DEBUG] GS.ADProAuthentication.View - ==== Current UserID is: -1
[Thread:11][DEBUG] GS.ADProAuthentication.View - Session.SessionID: u0ycfcoxiwdkd5negqcqg4xe
[Thread:11][DEBUG] GS.ADProAuthentication.View - Session.CodePage: 65001
[Thread:11][DEBUG] GS.ADProAuthentication.View - Session.CookieMode: UseCookies
[Thread:11][DEBUG] GS.ADProAuthentication.View - Session.IsCookieless: False
[Thread:11][DEBUG] GS.ADProAuthentication.View - Session.IsNewSession: True
[Thread:11][DEBUG] GS.ADProAuthentication.View - Session.IsReadOnly: False
[Thread:11][DEBUG] GS.ADProAuthentication.View - Session.IsSynchronized: False
[Thread:11][DEBUG] GS.ADProAuthentication.View - Session.LCID (locale identifier): 1033
[Thread:11][DEBUG] GS.ADProAuthentication.View - Session.Mode: InProc
[Thread:11][DEBUG] GS.ADProAuthentication.View - Session.Timeout (minutes): 20
[Thread:11][DEBUG] GS.ADProAuthentication.View - LogonUserIdentity name: IIS APPPOOL\Intranet, auth type:
[Thread:11][DEBUG] GS.ADProAuthentication.View - Request.LogonUserIdentity.Groups: S-1-1-0 |S-1-5-32-545 |
[Thread:11][DEBUG] GS.ADProAuthentication.View - Module version: 3.2.0
[Thread:11][DEBUG] GS.ADProAuthentication.View - DNN Domain: http://my-domain.com:80
[Thread:11][DEBUG] GS.ADProAuthentication.View - Portal id: 0
[Thread:11][DEBUG] GS.ADProAuthentication.View - Text box username: not found
[Thread:11][DEBUG] GS.ADProAuthentication.View - Windows Authentication LOGON_USER: not found
[Thread:11][DEBUG] GS.ADProAuthentication.View - ActualConnectionString: CAREE LDAP://192.168.3.156
[Thread:11][DEBUG] GS.ADProAuthentication.View - List of all available AD-Pro Auth connection strings: CAR
[Thread:11][DEBUG] GS.ADProAuthentication.View - List of all available AD-Pro Auth connection strings read
[Thread:11][DEBUG] GS.ADProAuthentication.View - RedirectURL: /
[Thread:11][DEBUG] GS.ADProAuthentication.View - Previous page: not found
```

Logs are created only when plugin is working in “Diagnostic Mode”, to enable it please follow steps below:

1. Open log4net configuration file `DotNetNuke.log4net.config`, it can be found in DNN root folder, see figure below:

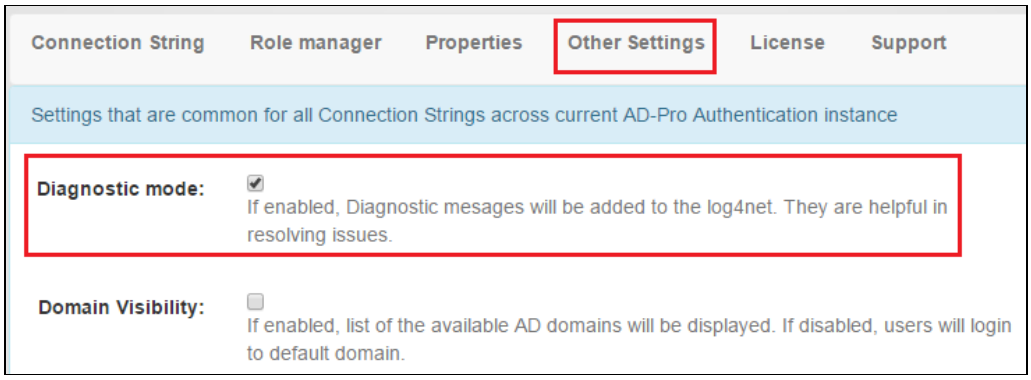


Portals	09/19/16 14:59	File folder
Providers	09/19/16 14:46	File folder
Resources	09/19/16 14:46	File folder
51Degrees.mobi.config	09/19/16 14:46	XML Configuratio...
403-3.gif	01/14/16 11:37	IrfanView GIF File
compilerconfig.json	01/14/16 11:38	JSON File
Default.aspx	01/14/16 11:37	ASP.NET Server Pa...
DNN.ico	01/14/16 11:37	IrfanView ICO File
DotNetNuke.config	01/14/16 11:37	XML Configuratio...
DotNetNuke.log4net.config	06/05/18 15:52	XML Configuratio...
ErrorPage.aspx	01/14/16 11:37	ASP.NET Server Pa...
favicon.ico	01/14/16 11:38	IrfanView ICO File
Global.asax	01/14/16 11:37	ASP.NET Server A...
jquery.min.map	01/14/16 11:38	Linker Address Map

2. Inside that file set log level to `ALL`, see code snippet below:

```
<root>
    <level value="ALL" />
    <appender-ref ref="RollingFile" />
</root>
```

3. Open “AD-Pro Authentication-> Module options-> Other Settings” tab and enable attribute “Diagnostic Mode”, see figure below



4. Now logging mechanism is turned on, reproduce the sign-in process and check the log file.

10.2. How generate diagnostic logs

Please follow the instructions below on how to generate valuable logs.

1. First enable diagnostic mode, to do that see instructions from section Diagnostic Mode

2. Log file is usually very big, which makes it difficult to parse. To remove unncecessary informations, delete log file, before you will reproduce the issue.

   Default path to log file is: `~\Portals\_default\Logs\YYYY.MM.DD.resoures`

3. Reproduce the issue to generate log entries.

4. Compress log file, and send it to support@glanton.com

10.3. JavaScript issues

10.3.1. Overview

User interface is created at the top of AngularJS framework. JavaScript can be moody although it's very fast. If you will see interface issues, for example view can't be loaded or displayed, buttons aren't responding, it's worth to check JavaScript errors. Depending what browser you are using, check following articles that are describing how to display these errors in your browser:

- ⇗display JavaScript errors in Chrome
- ⇗display JavaScript errors in FireFox
- ⇗display JavaScript errors in Internet Explorer

If you have any problems with your plugin, please send above error messages to support@glanton.com

10.3.2. Edit & Delete buttons doesn't work

When you can't update module settings, and JavaScript throws error like `Method Not Allowed...` or requests throws `405 HTTP` error code, please make sure that `WebDAV` is disabled. To disable `WebDAV`, please add following lines to the `web.config` file, in the section `system.webServer-> modules` add following line:

```
<modules>
    <remove name="WebDAVModule"/> <!-- add this -->
    ...
</modules>
```

in the section `system.webServer-> handlers` add following line:

```
<handlers>
    <remove name="WebDAV" />
    ...
</handlers>
```

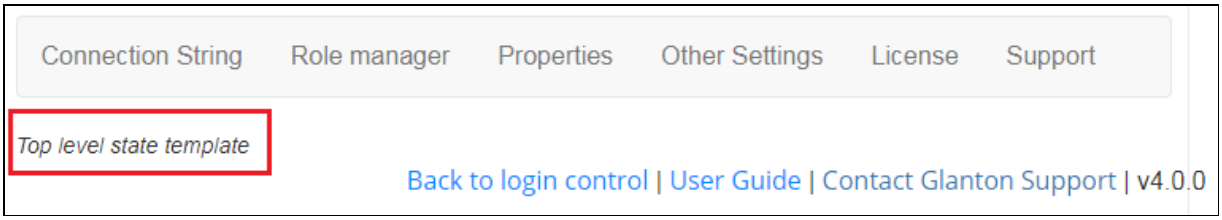
the `ExtensionlessUrl-Integrated-4.0` handler under the `system.webServer-> handlers` also applies the verb `PUT`:

```
<handlers>
    ...
    <remove name="ExtensionlessUrl-Integrated-4.0" />
    <add name="ExtensionlessUrl-Integrated-4.0" path="*." verb="GET,HEAD,POST,DEBUG,PUT,DELETE" type="System.Web.Handlers.Tra
    ...
</handlers>
```

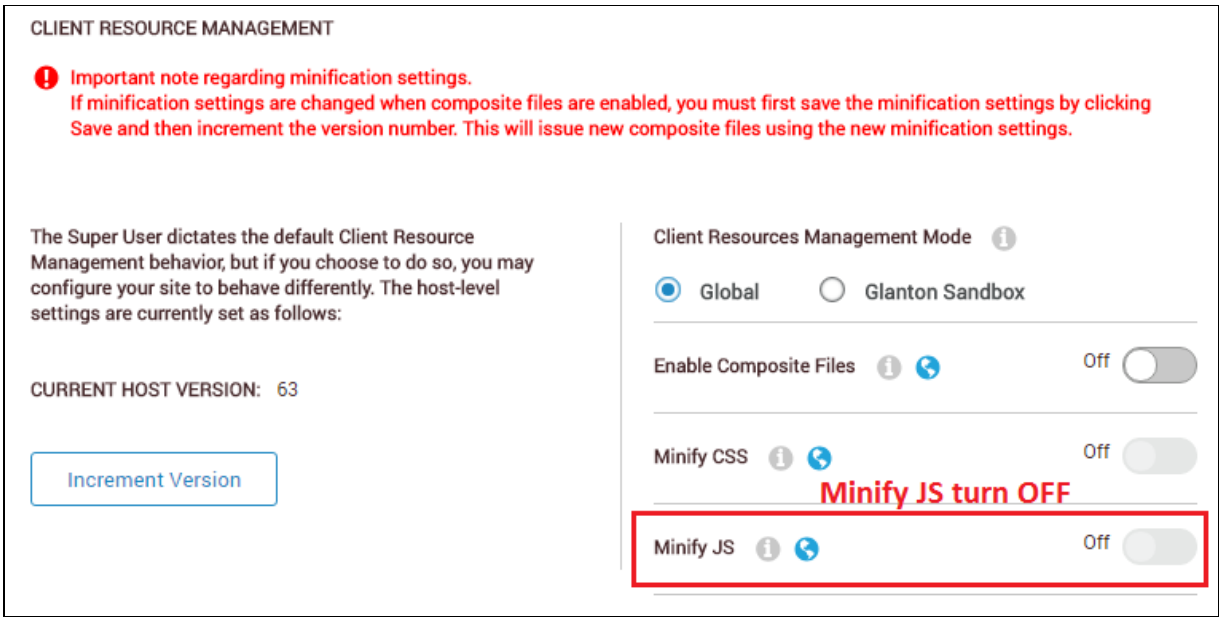
⇗Here you can read more about WebDAV.

10.3.3. View can't be loaded

If you see situation like on figure below, where only upper part of interface is loaded and instead of bottom part of interface is displayed message `Top level state template`, probably it's caused by minified js file.



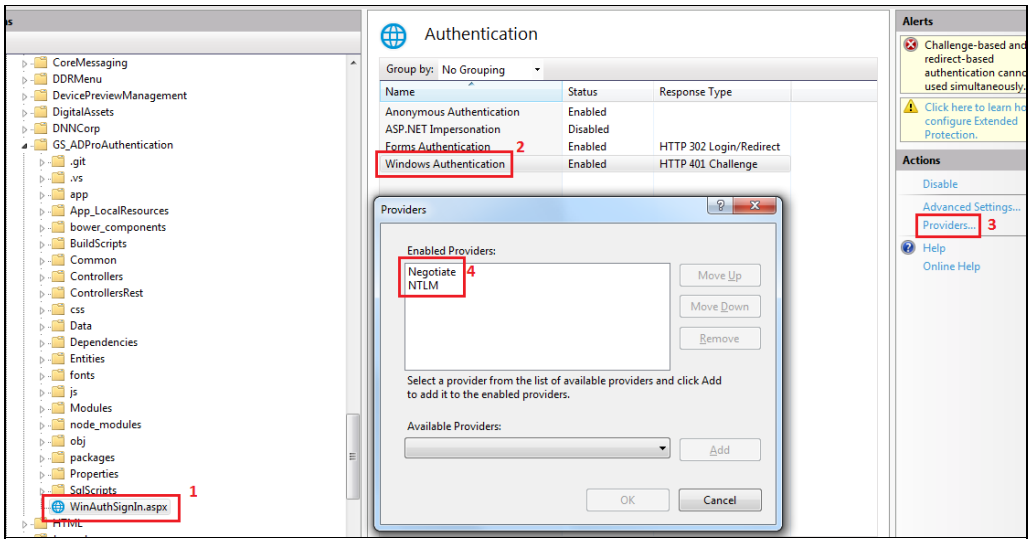
To fix that issue sign in as DNN host and go to menu "Servers-> Server Settings". At the bottom is section responsible for reducing Java Script files, please disable `Minify JS` attribute. See figure below for more info.



10.4. SSO - providers order

When all configuration steps for the SSO was done, but you keep getting windows popup asking you to enter user credentials, possible it's worth to change providers order.

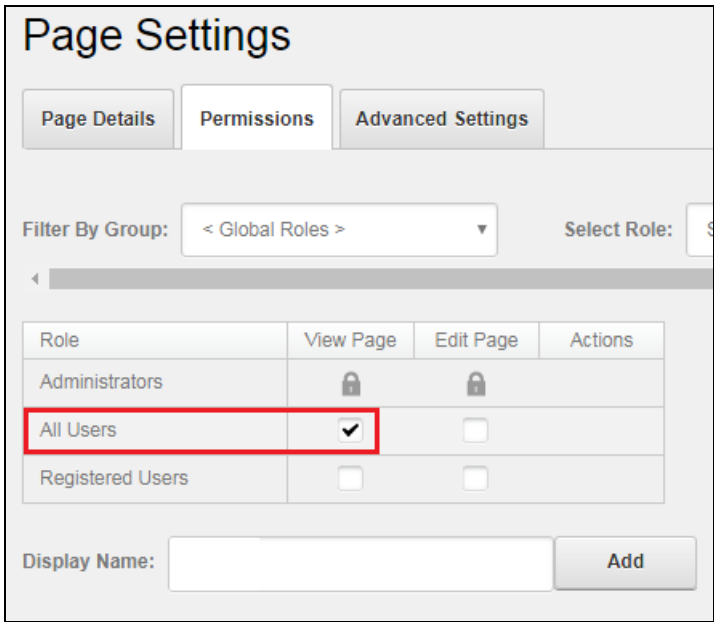
1. Go to IIS and open `Authentication` tab for the `~\DesktopModules\GS_ADProAuthentication\WinAuthSignIn.aspx` file.
2. Select `Windows Authentication`.
3. Click on `Providers`.
4. Inside popup `Providers`, swap places for `Negotiate` and `NTLM`.
5. Apply settings by clicking on `OK` button, see figure below:



Before you test SSO make sure that cache is deleted in IIS, DNN and web browser.

10.5. Log off issues

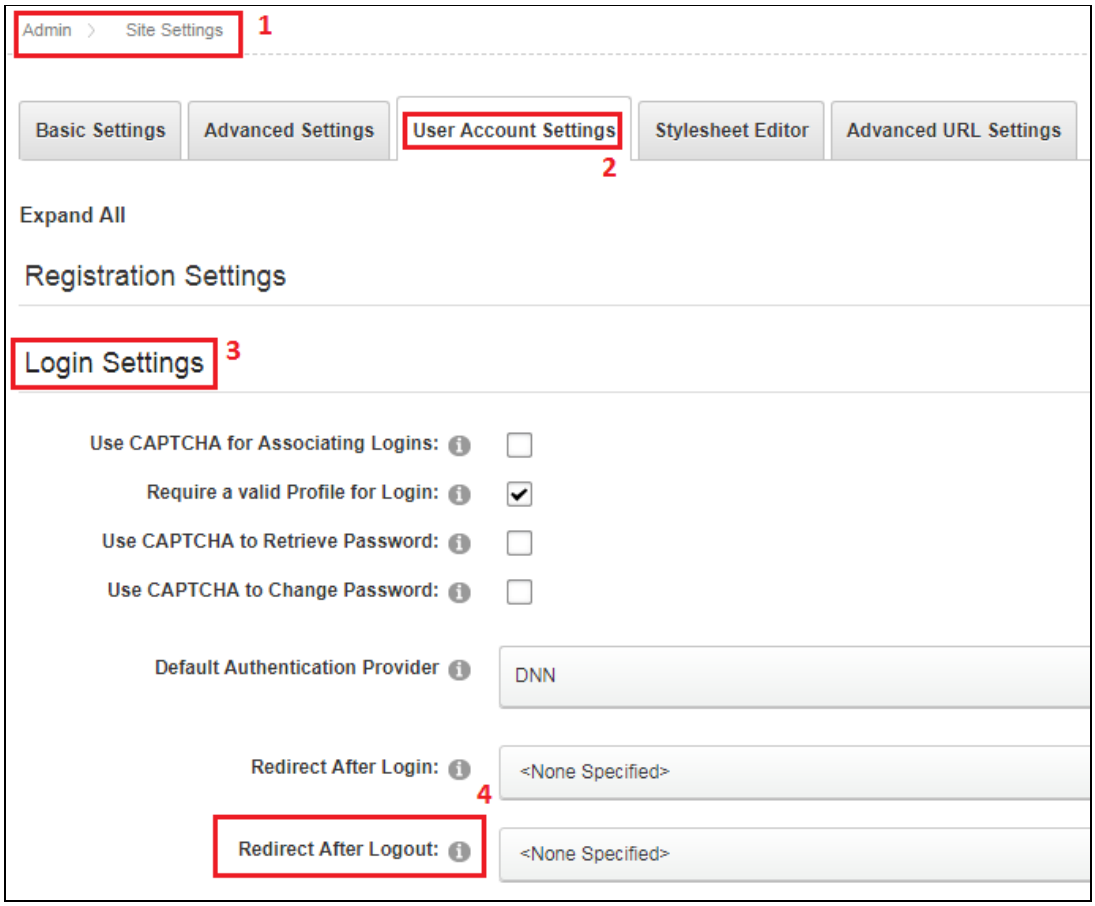
If there are any issues at the sign off process, it's worth to consider set dedicated log off page. It's important that log off page should have permissions `View Page` for `All Users`, see image below.



To set up custom log off page follow steps below:

1. Sign in to DNN as Admin or Host.
2. Go to `Admin->Site Settings`
3. Select `User Account Settings` tab, then `Login Settings` section.
4. Under `Redirect After Logout` attribute, set new log off page.

See figure below for more info:



11. Release Notes

- Version 04.00.00
    - 06/24/2018 [+] added option to validate LDAP connection
- Version 03.05.00
    - 06/08/2016 [!] fixed bug when SSO session was unexpectedly expired
    - 05/18/2016 [+] improved 'Diagnostic Mode'
    - 03/08/2016 [+] when in 'Role Manager', 'Authorization Role' is enabled, all child roles are also automatically enabled
    - 03/15/2016 [!] fixed bug when DNN user was added to the new DNN role
    - 03/17/2016 [+] added ability to change Active Directory user password
- Version 03.03.00
    - 03/06/2016 [!] fixed bug when AD user wasn't validated when LDAP was using SSL mode
- Version 03.02.00

    - 21/10/2015 [+] module works with custom HTTTP ports
    - 23/10/2015 [+] module works when DNN site has only 'Windows Authentication' enabled

- Version 03.01.00
    - 10/10/2015 [+] added ability to sync Active Directory user profile photo

End User License Agreement for "AD-Pro Authentication" extension

This is a CONTRACT between you (either an individual or a single entity) and GLANTON, which covers your use of "ADPro Authentication" and related software components. All such software is referred to herein as the "Software Product." A software license is issued to a designated user only by GLANTON or its authorized agents. If you do not agree to the terms of this EULA, then do not install or use the Software Product or the Software Product License. By explicitly accepting this End-User License Agreement (EULA) you are acknowledging and agreeing to be bound by the following terms:

Installation and Use

Trial License You may install each Software Product License on a single non-Production DotNetNuke Instance for the period of the Trial License.

Standard License You may install each Software Product License on a single Production DotNetNuke Instance. This Software Product License is valid for non-Production copies of the DotNetNuke instance including those used for development, acceptance testing, staging, web farm and disaster recovery instances of the Production DotNetNuke instance.

This Software Product License is valid for all child Dotnetnuke portals configured on the Production DotNetNuke instance and which are all owned by the same user or legal entity.

Summary of this EULA

1. Trial copies may only be used to determine suitability.
2. License for use is a non-exclusive, non transferable right.
3. You may install the Software Product License on a single Production DotNetNuke® Instance.
4. You may install the Software Product License on all child Dotnetnuke portals configured on the Production DotNetNuke instance and which are all owned by the same user or legal entity
5. The Software Product is owned by GLANTON and is protected by United Kingdom and international copyright laws.
6. You may not rent, lease, lend, or in any way distribute or transfer any rights in this EULA or the Software Product to third parties without GLANTON's written approval.
7. You hereby agree to indemnify GLANTON against and hold harmless GLANTON from any claims.
8. Any software provided along with the Software Product that is associated with a separate license agreement.
9. GLANTON may provide you with support services related to the Software Product.
10. GLANTON may terminate this EULA and Revoke the License if you fail to comply with any term or condition of this EULA.
11. Export of Software Product is limited to that allowable by law.
12. YOU ACCEPT THE SOFTWARE PRODUCT AND SOFTWARE PRODUCT LICENSE "AS IS".

13. Limitation of liability.

14. High risk activities.

15. Governing Law; Entire Agreement; Dispute Resolution.

16. If any provision of this EULA is held invalid, the remainder of this EULA shall continue in full force and effect.

17. If you are located outside the U.S., then the provisions of this Section shall apply.

1. EVALUATION/TRIAL LICENSE WARNING

This Software Product under special circumstances may be used in conjunction with a free evaluation/trial Software Product License. If you are using such an evaluation/trial Software Product License, you may use the Software Product only to evaluate its suitability for purchase. Evaluation/Trial Software has been limited in some way either through timeouts, disabled save or restricted use.

GLANTON BEARS NO LIABILITY FOR ANY DAMAGES RESULTING FROM USE (OR ATTEMPTED USE AFTER EXPIRATION) OF THE SOFTWARE PRODUCT AND HAS NO DUTY TO PROVIDE ANY SUPPORT BEFORE OR AFTER THE EXPIRATION DATE OF AN EVALUATION LICENSE.

2. GRANT OF NON-EXCLUSIVE LICENSE

GLANTON grants the non-exclusive, non-transferable right for a single user, or entity to use this Software Product. Each additional user or entity of the Software Product requires an additional Software Product License. An entity is defined as any company, association, or organization.

When the source code is provided with the Software Product, GLANTON grants you the right to modify, alter, improve, or enhance the Software Product without limitation, except as described in this EULA.

Although rights to modification of the Software Product are granted by this EULA, you may not tamper with, alter, or use the Software Product in a way that disables, circumvents, or otherwise defeats its built-in licensing verification and enforcement capabilities. The right to modification of the Software Product also does not include the right to remove or alter any trademark, logo, copyright or other proprietary notice, legend, symbol or label in the Software Product.

Any modifications made to the Software Product will render it non-supportable by GLANTON. You may, at your discretion, contact GLANTON about distribution of the altered Software Product, and if agreeable terms can be determined, the software product may be distributed according to the agreement. The altered Software Product will become supported by the party designated in the agreement between GLANTON and the user. Ownership of the altered SOFTWARE PRODUCT is transferred to the party designated in the agreement between GLANTON and the user. You may not distribute or redistribute changes made to the Software Product to anyone other than groups designated by the agreement between GLANTON and the user. Contact GLANTON using the information included at the end of this document.

Although the source code for the Software Product may be included, you may not share, use, or reuse the knowledge or technologies in other applications without explicit approval from GLANTON.

You may make copies of the Software Product as is reasonably necessary for its use. Each copy must reproduce all copyright and other proprietary rights notices on or in the Software Product.

You may install each Software Product License on a single Host DotNetNuke Instance. You may also make copies of the Software Product License as necessary for backup and/or archival purposes. Backup and archival copies may not come into active use with the Software Product for any purpose. No other copies may be made.

You may install this Software Product in any number of Host DotNetNuke Instances running only on the local computer IP adddress which cannot be accessed by any remote computer.

Each copy must reproduce all copyright and other proprietary rights notices on or in the Software Product License. You may not modify or create derivative copies of the Software Product License.

All rights not expressly granted to you are retained by GLANTON.

3. INTELLECTUAL PROPERTY RIGHTS RESERVED BY GLANTON

The Software Product is owned by GLANTON and is protected by United Kingdom and international copyright laws and treaties, as well as other intellectual property laws and treaties. You must not remove or alter any copyright notices on any copies of the Software Product. This Software Product copy is licensed, not sold. You may not use, copy, or distribute the Software Product, except as granted by this EULA, without written authorization from GLANTON or its designated agents. Furthermore, this EULA does not grant you any rights in connection with any trademarks or service marks of GLANTON. GLANTON reserves all intellectual property rights, including copyrights, and trademark rights.

4. LICENSED FOR ONE PRODUCTION DOTNENUKE INSTANCE

Standard License: You may install each Software Product License on a single Production DotNetNuke Instance. This Software Product License is valid for non-Production copies of the DotNetNuke instance including those used for development, acceptance testing, staging, web farm and disaster recovery instances of the Production DotNetNuke instance. This Software Product License is valid for all child Dotnetnuke portals configured on the Production DotNetNuke instance and which are all owned by the same user or legal entity.

Additional Domain Name extension Licenses may be obtained either singly or in bundles.

Any attempts to defeat the Domain Name verification and Unlicensed message may invalidate the license in it's entirety at the sole discretion of GLANTON

5. NO RIGHT TO TRANSFER

You may not rent, lease, lend, or in any way distribute or transfer any rights in this EULA or the Software Product to third parties without GLANTON's written approval, and subject to written agreement by the recipient of the terms of this EULA.

6. INDEMNIFICATION

You hereby agree to indemnify GLANTON against and hold harmless GLANTON from any claims, lawsuits or other losses that arise out of your breach of any provision of this EULA.

7. THIRD PARTY RIGHTS

Any software provided along with the Software Product that is associated with a separate license agreement is licensed to you under the terms of that license agreement. This license does not apply to those portions of the Software Product. Copies of these third party licenses are included in all copies of the Software Product.

8. SUPPORT SERVICES

GLANTON may provide you with support services related to the Software Product. Use of any such support services is governed by GLANTON policies and programs described in online documentation and/or other GLANTON-provided materials.

As part of these support services, GLANTON may make available bug lists, planned feature lists, and other supplemental informational materials.

GLANTON MAKES NO WARRANTY OF ANY KIND FOR THESE MATERIALS AND ASSUMES NO LIABILITY WHATSOEVER FOR DAMAGES RESULTING FROM ANY USE OF THESE MATERIALS. FURTHERMORE, YOU MAY NOT USE ANY MATERIALS PROVIDED IN THIS WAY TO SUPPORT ANY CLAIM MADE AGAINST GLANTON.

Any supplemental software code or related materials that GLANTON provides to you as part of the support services, in periodic updates to the Software Product or otherwise, is to be considered part of the Software Product and is subject to the terms and conditions of this EULA.

With respect to any technical information you provide to GLANTON as part of the support services, GLANTON may use such information for its business purposes without restriction, including product support and development. GLANTON Inc. will not use such technical information in a form that personally identifies you without first obtaining your permission.

9. TERMINATION WITHOUT PREJUDICE TO ANY OTHER RIGHTS

GLANTON may terminate this EULA and Revoke the License if you fail to comply with any term or condition of this EULA. In such event, you must destroy all copies of the Software Product and Software Product Licenses.

10. NO WARRANTIES

YOU ACCEPT THE SOFTWARE PRODUCT AND SOFTWARE PRODUCT LICENSE "AS IS," AND GLANTON AND ITS THIRD PARTY SUPPLIERS AND LICENSORS MAKE NO WARRANTY AS TO ITS USE, PERFORMANCE, OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, GLANTON AND ITS THIRD PARTY SUPPLIERS AND LICENSORS DISCLAIM ALL OTHER REPRESENTATIONS, WARRANTIES, AND CONDITIONS, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE PRODUCT REMAINS WITH YOU.

11. LIMITATION OF LIABILITY

THIS LIMITATION OF LIABILITY IS TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. IN NO EVENT SHALL GLANTON OR ITS THIRD PARTY SUPPLIERS AND LICENSORS BE LIABLE FOR ANY COSTS OF SUBSTITUTE PRODUCTS OR SERVICES, OR FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THIS EULA OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF GLANTON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, GLANTON'S, AND ITS THIRD PARTY SUPPLIERS' AND LICENSORS', ENTIRE LIABILITY ARISING OUT OF THIS EULA SHALL BE LIMITED TO THE LESSER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT OR THE PRODUCT LIST PRICE; PROVIDED, HOWEVER, THAT IF YOU HAVE ENTERED INTO A GLANTON SUPPORT SERVICES AGREEMENT, GLANTON'S ENTIRE LIABILITY REGARDING SUPPORT SERVICES SHALL BE GOVERNED BY THE TERMS OF THAT AGREEMENT.

12. HIGH RISK ACTIVITIES

The Software Product is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Software Product, or any software, tool, process, or service that was developed using the Software Product, could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). Accordingly, GLANTON and its suppliers and licensors specifically disclaim any express or implied warranty of fitness for High Risk Activities. You agree that GLANTON and its suppliers and licensors will not be liable for any claims or damages arising from the use of the Software Product, or any software, tool, process, or service that was developed using the Software Product, in such applications.

13. GOVERNING LAW; ENTIRE AGREEMENT; DISPUTE RESOLUTION

This EULA is governed by the laws of the Queensland, Australia.

This EULA is the entire agreement between GLANTON and you, and supersedes any other communications or advertising with respect to the Software Product. This EULA may be modified only by written agreement signed by authorized representatives of you and GLANTON.

Unless otherwise agreed in writing, all disputes relating to this EULA (except any dispute relating to intellectual property rights) shall be subject to final and binding arbitration in England, the United Kingdom . If any dispute arises under this EULA, the prevailing party shall be reimbursed by the other party for any and all legal fees and costs associated therewith.

16. SEVERABILITY

If any provision of this EULA is held invalid, the remainder of this EULA shall continue in full force and effect.

A waiver by either party of any term or condition of this EULA or any breach thereof, in any one instance, shall not waive such term or condition or any subsequent breach thereof.

17. CONTACT INFORMATION

If you have any questions about this EULA, or if you want to contact GLANTON for any reason, please direct all correspondence to: support@glanton.com