Shield

Umbraco active security modules

# Installation

### Installing via Nuget

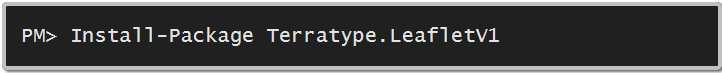
This Umbraco package can be installed via Nuget

The first part is the Shield framework, which coordinates the different security apps, which can be found here

<https://www.nuget.org/packages/Our.Shield.Core/>



And the second part is the Shield apps, which provides the active security. Note, there are no restriction on the number of shield apps that can be installed. If you want, install them all using Nuget, to gain the full benefits of what Shield can provide.

* **Backoffice Access**   
  Gives you the ability to configure the backoffice access URL and restricts access to your desired URL via a white-list of IP Addresses.  
    
  <https://www.nuget.org/packages/Our.Shield.BackofficeAccess>  
    
  
* Media Protection  
  Provides you the ability to disable [Hotlinking](https://simple.wikipedia.org/wiki/Hotlinking) and to secure your media to only be accessed by authenticated members.  
    
  <https://www.nuget.org/packages/Our.Shield.MediaProtection>  
    
  

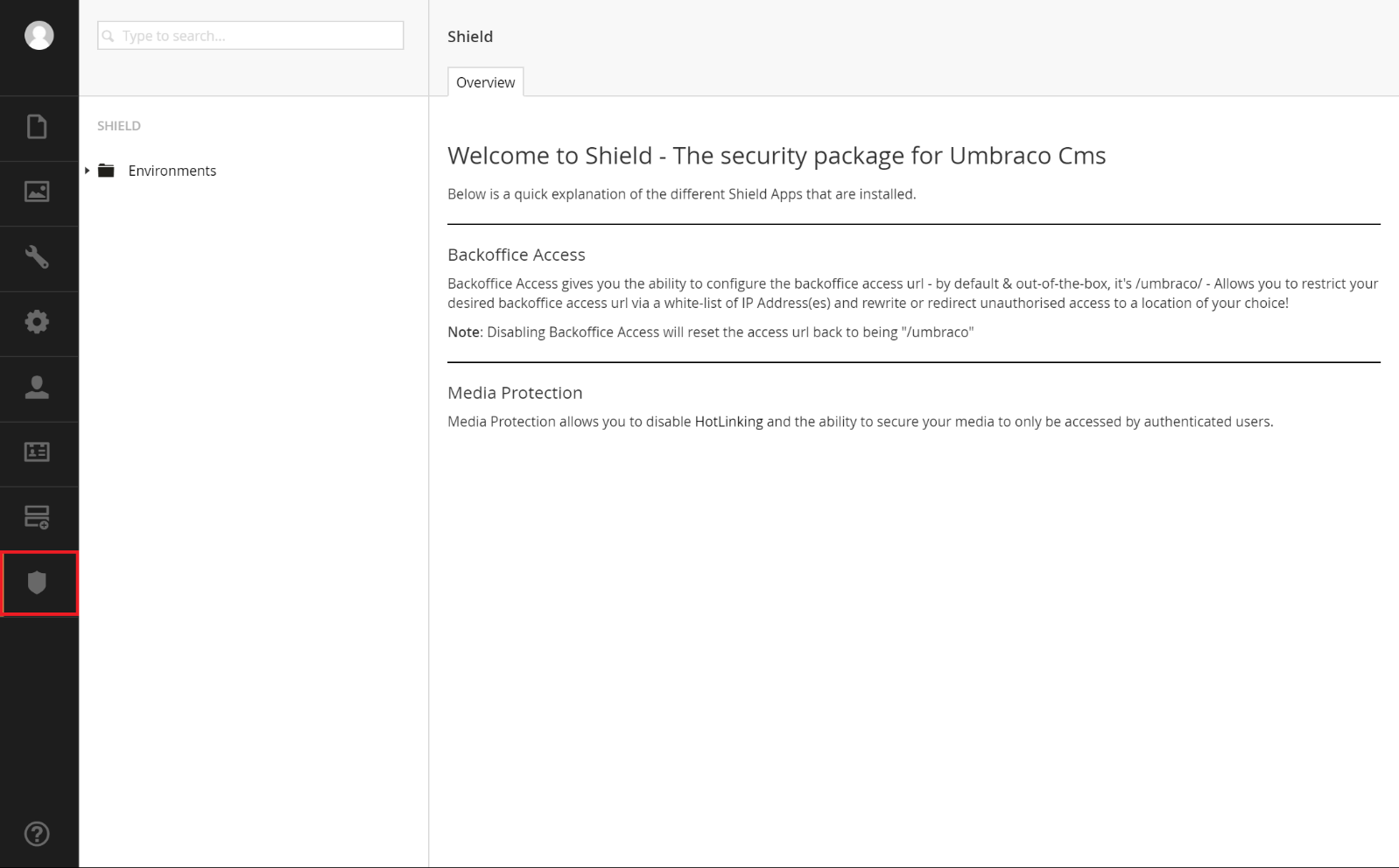
### Installing via Umbraco Package Manager

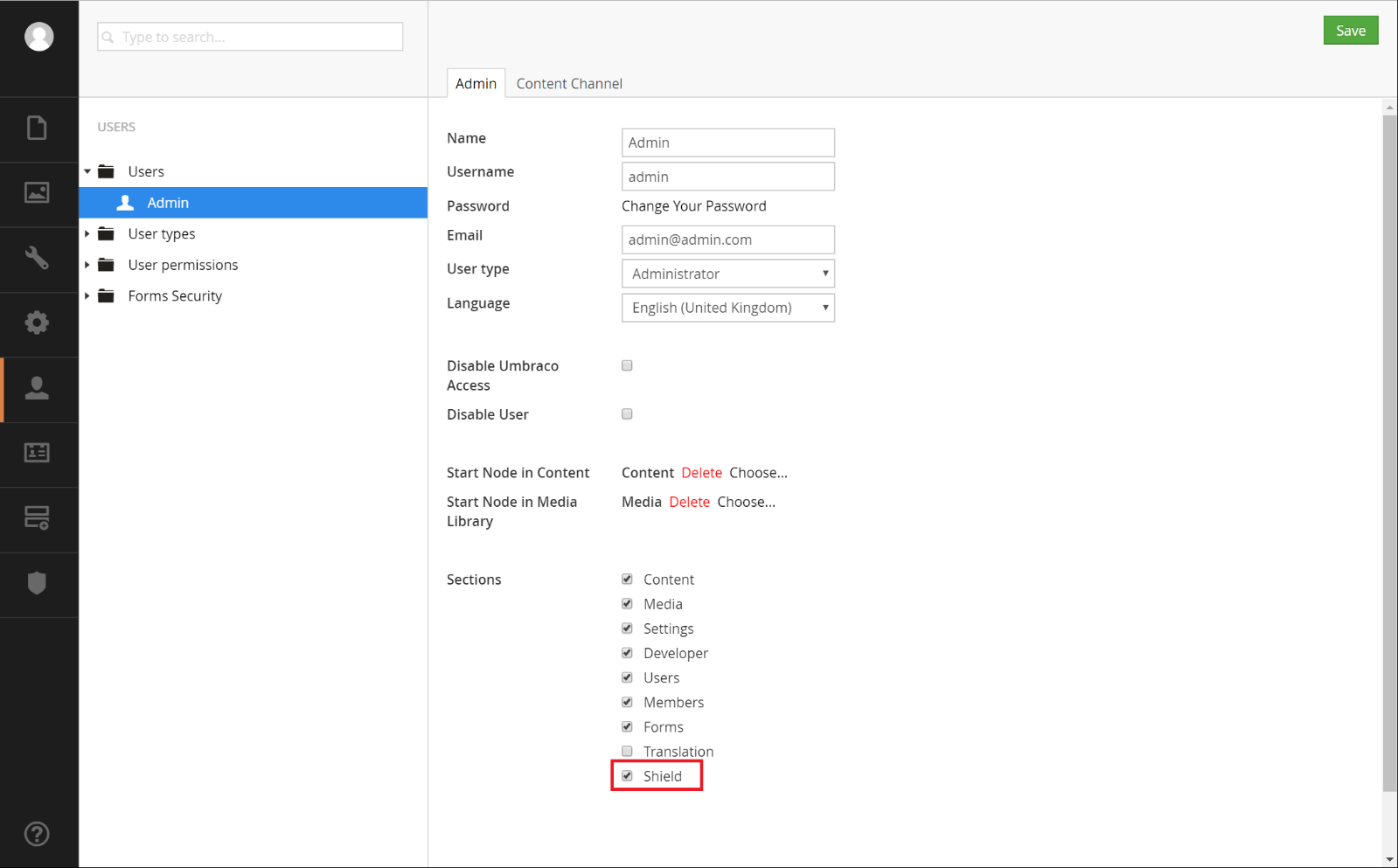
[https://our.umbraco.org/projects/backoffice-extensions/Our.Shield/](https://our.umbraco.org/projects/backoffice-extensions/terratype/)

This installation contains the Shield framework, and all available Shield apps

# Our.Shield.Core

Our.Shield.Core is the framework for the Our.Shield Umbraco package. It contains the custom section to be displayed in Umbraco and does the ‘heavy’ lifting for the installed app(s).

Once installed, you should see a new custom section within the backoffice of Umbraco.

If the new section doesn’t display, you’ll need to allow the currently logged in user to have access to the Shield section via the users’ section:

## Environments Node

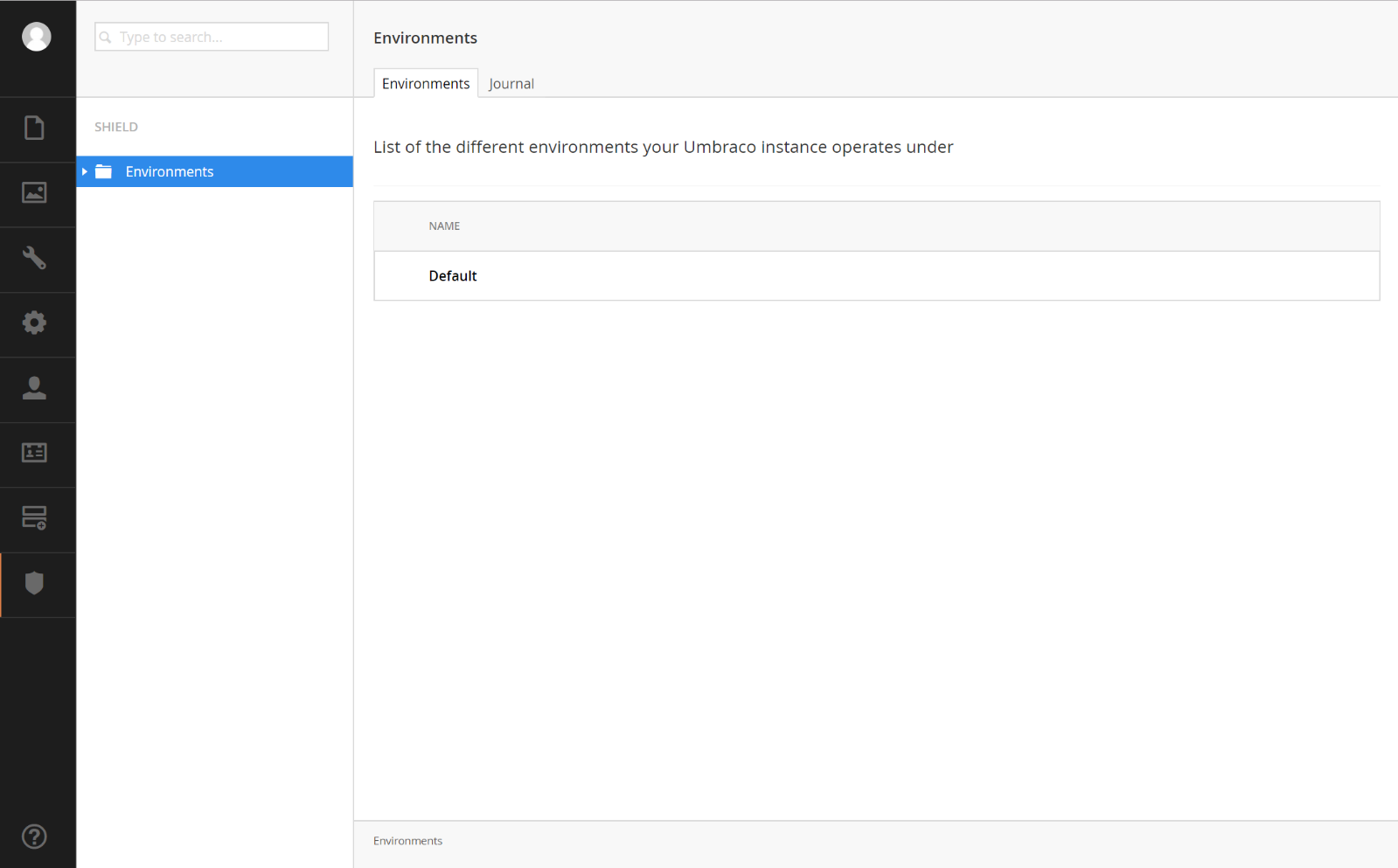
The Environments node will display all configured environments on the “Environments” tab and a Journal on the “Journal” tab, see below for an explanation of these 2 tabs.

### Environments Tab

The environments tab will display a table listing the environments that have been created. By default, there will be a “Default” environment when Shield is installed against an Umbraco installation. At present, there isn’t the ability to create more environment(s) for Shield. This will be coming in the next release of Shield. The purpose of an environment will allow you to have different Shield apps that are installed to be configured differently dependant on the environment’s purpose, with the ability to define the domain(s) that are for that environment. An example of an environment could be used in conjunction with the Backoffice Access shield app to define different white-list of IP addresses that can gain access to the configured backoffice access URL for the different sites, for example, say you have 2 websites within the same Umbraco installation:

1. site.com
2. site.co.uk

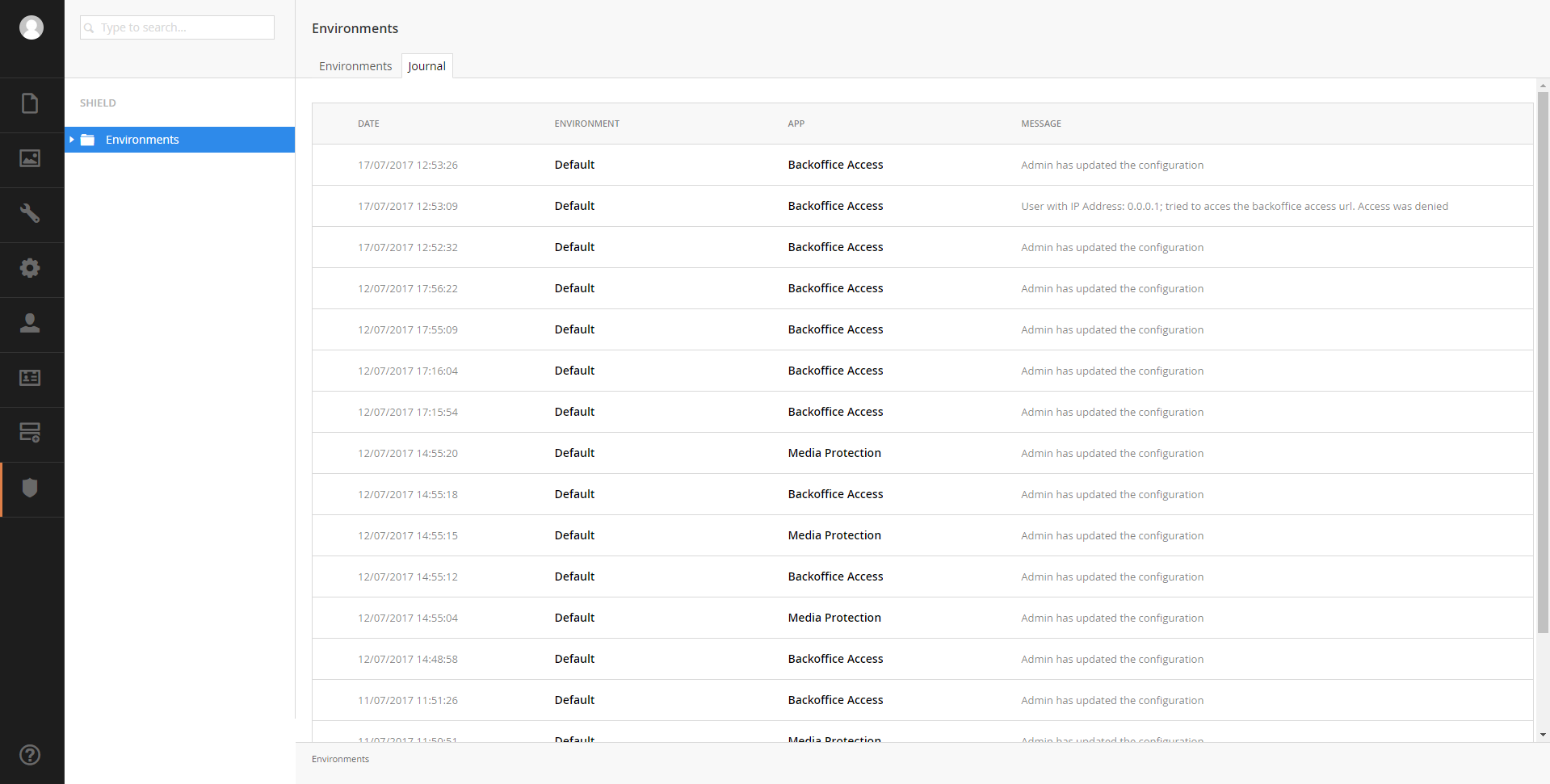
You could setup site.com to only allow Backoffice Access to those that can manage the site via a white-list of IP addresses, with a URL of “/admin/” and site.co.uk with a different white-list of IP addresses with a Backoffice Access URL of “/content/”.



### Journal Tab

The Journal tab will display all journal items (logs) that have been created by the different environment(s) & shield app(s). A Journal is composed of the following:

* Date & time of when the Journal item was created
* The environment of the app that created the Journal item
* The app that created the Journal item
* A message of why the Journal item was created.

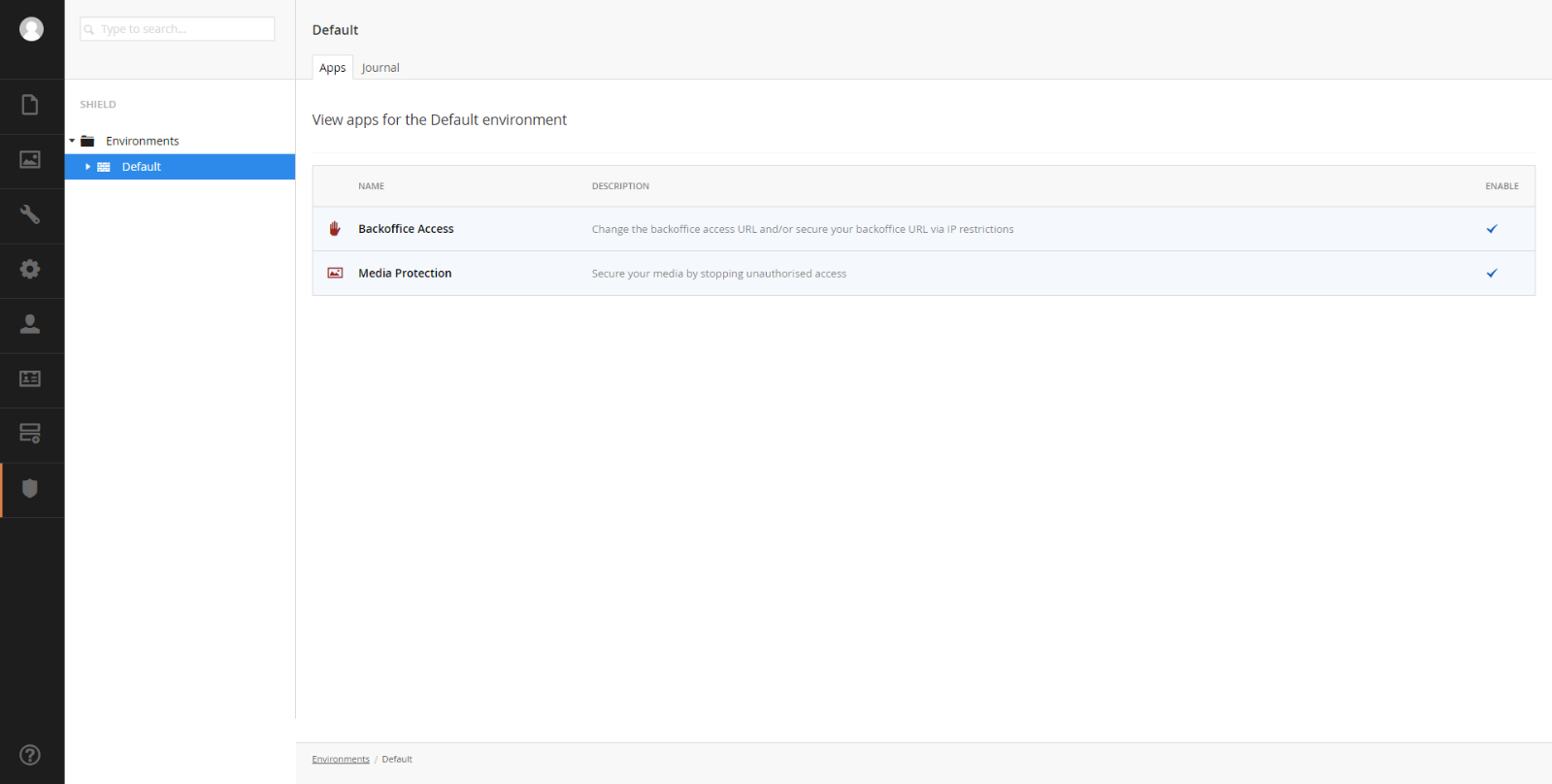


## Environment Node

The Environment node will display all installed apps on the “Apps” tab and a Journal on the “Journal” tab, see below for an explanation of these 2 tabs.

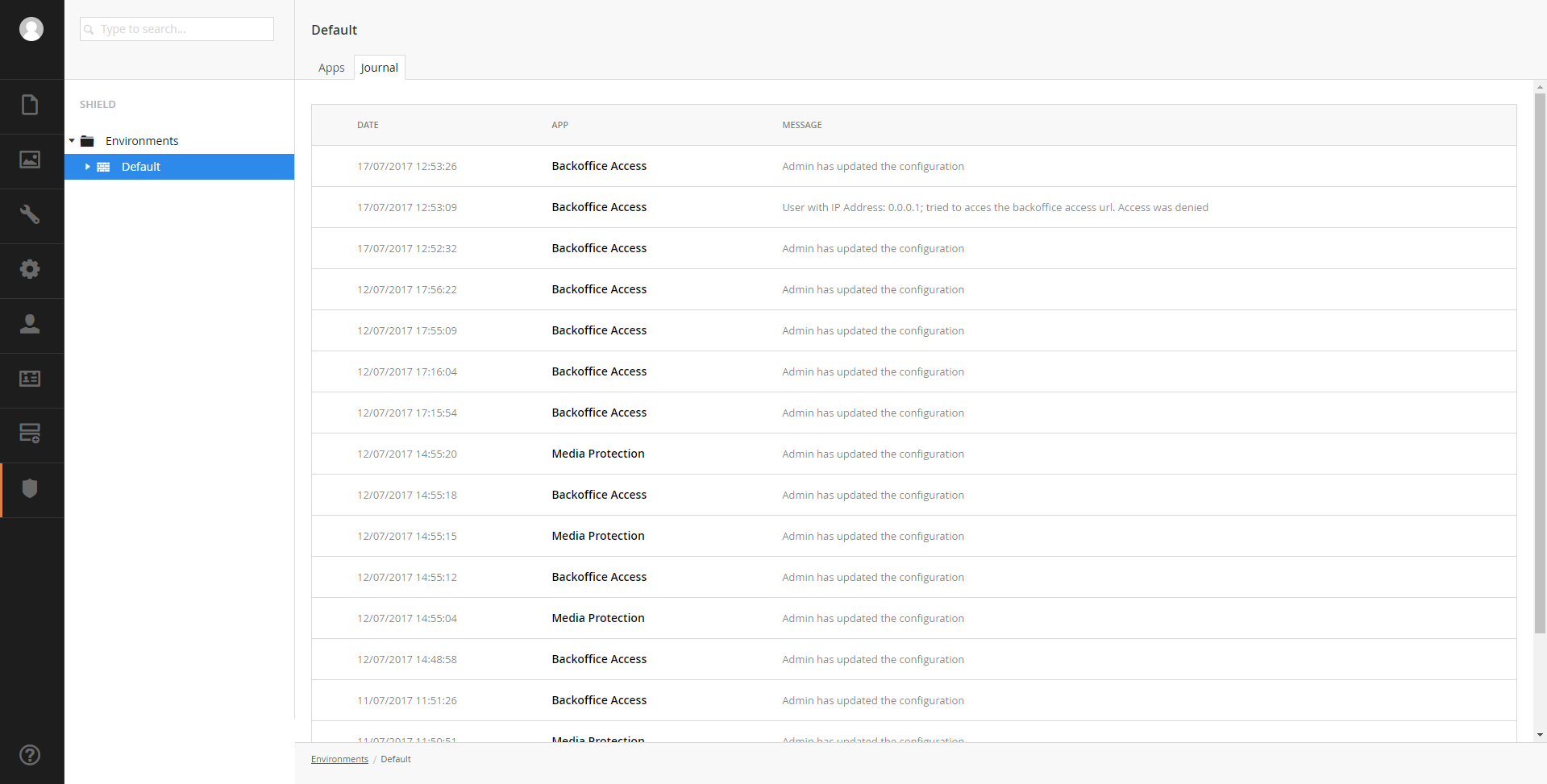
### Apps Tab

The Apps tab will display a listing of the Shield apps that are installed, showing the name, description and whether or not the app is enabled. Clicking on the app name will open up the app’s configuration.



### Journal Tab

Similar to the Environments node’s Journal tab, this will display the Journal items only for the selected environment. The difference being, the environment column is not included.



# Our.Shield.BackofficeAccess

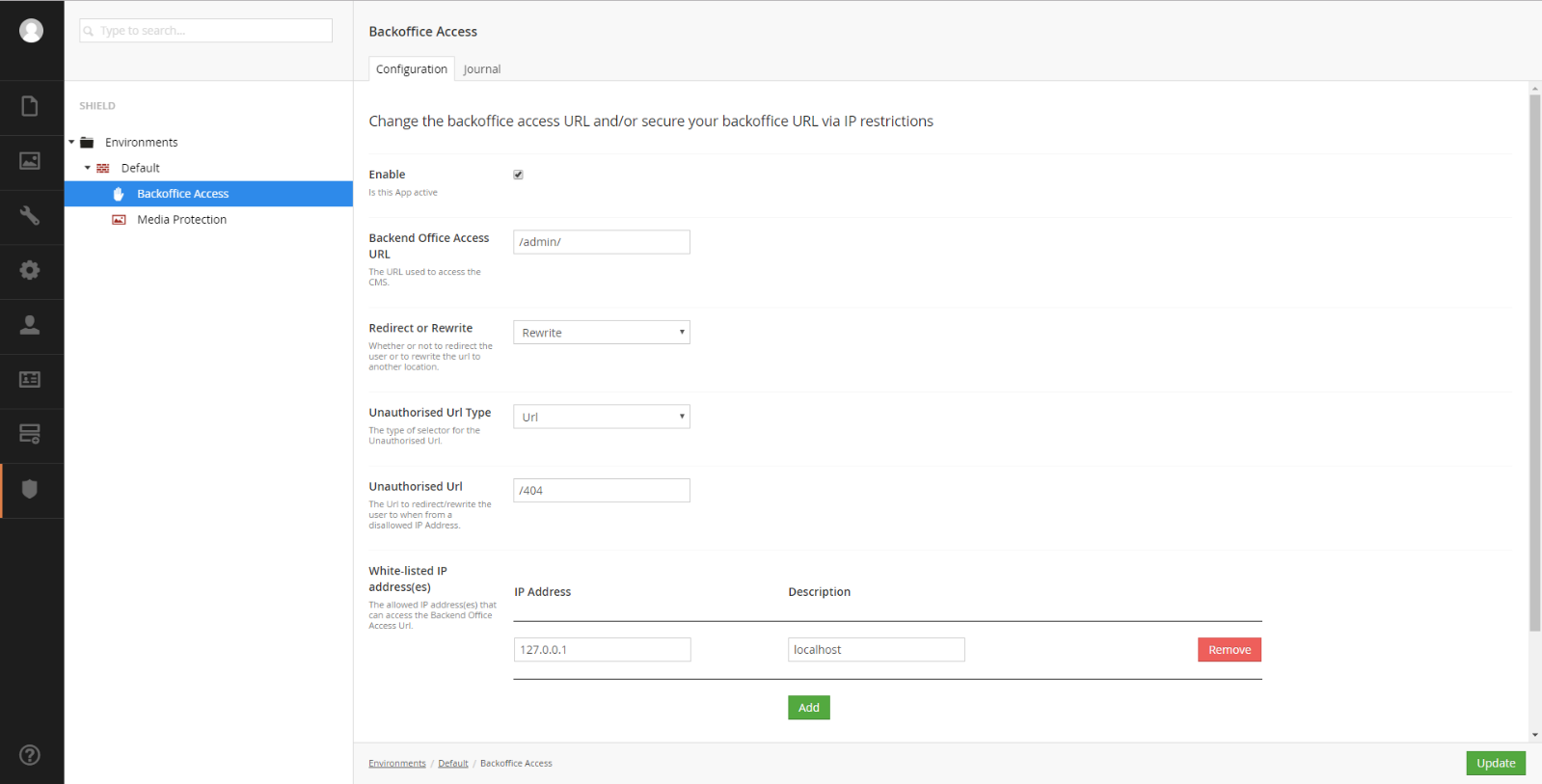
Once Backoffice Access has been installed, you should find a new node within the tree, or within the app listing on an environment node to access Backoffice Access’s Configuration and Journal.

Backoffice Access grants you the ability to change the backoffice access URL to a URL you desire, with the ability to restrict who can access the URL by a white-list of IP Addresses.

## Configuration Tab

The configuration gives you the ability to enable or disable the Shield app, configure the backoffice access URL (by default and out-of-the-box, it’s /umbraco/). The ability to redirect or rewrite unauthorised access to a location of your choice, with the ability to specify the location via:

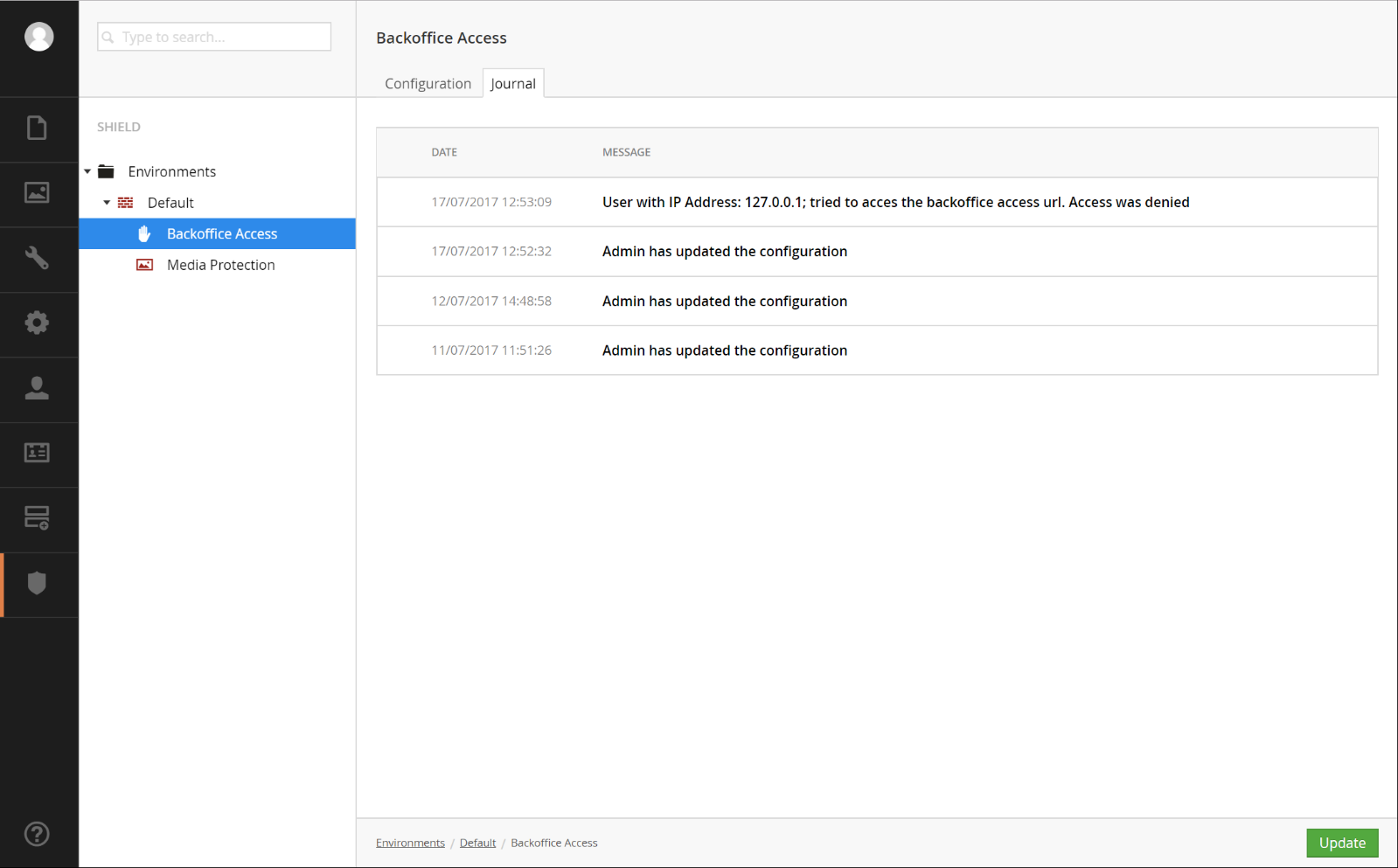
* URL – Textbox to allow you to specify the page. i.e. /404
* XPath – Textbox to allow you to specify the path to the page. i.e. //standardPage[@isDoc AND @nodeName=’404 Not Found’]  
  OR
* Content Picker – Provides you a content section content picker to select the desired page.



Lastly, the backoffice access configuration allows you to define a white-list of IP Addresses of whom can access the desired backoffice access URL – don’t forget to add localhost! You have the ability to specify the IP Addresses in IPv4 or IPv6 notation (with optionally specifying the cidr). For each white-listed IP address, you can optionally have a short description to identify what the IP address is for, so you don’t forget its purpose!

## Journal Tab

Similar to the other Journal tabs mentioned above, the difference being, only the selected app’s journal will be displayed, and the Environment/App columns are not displayed.



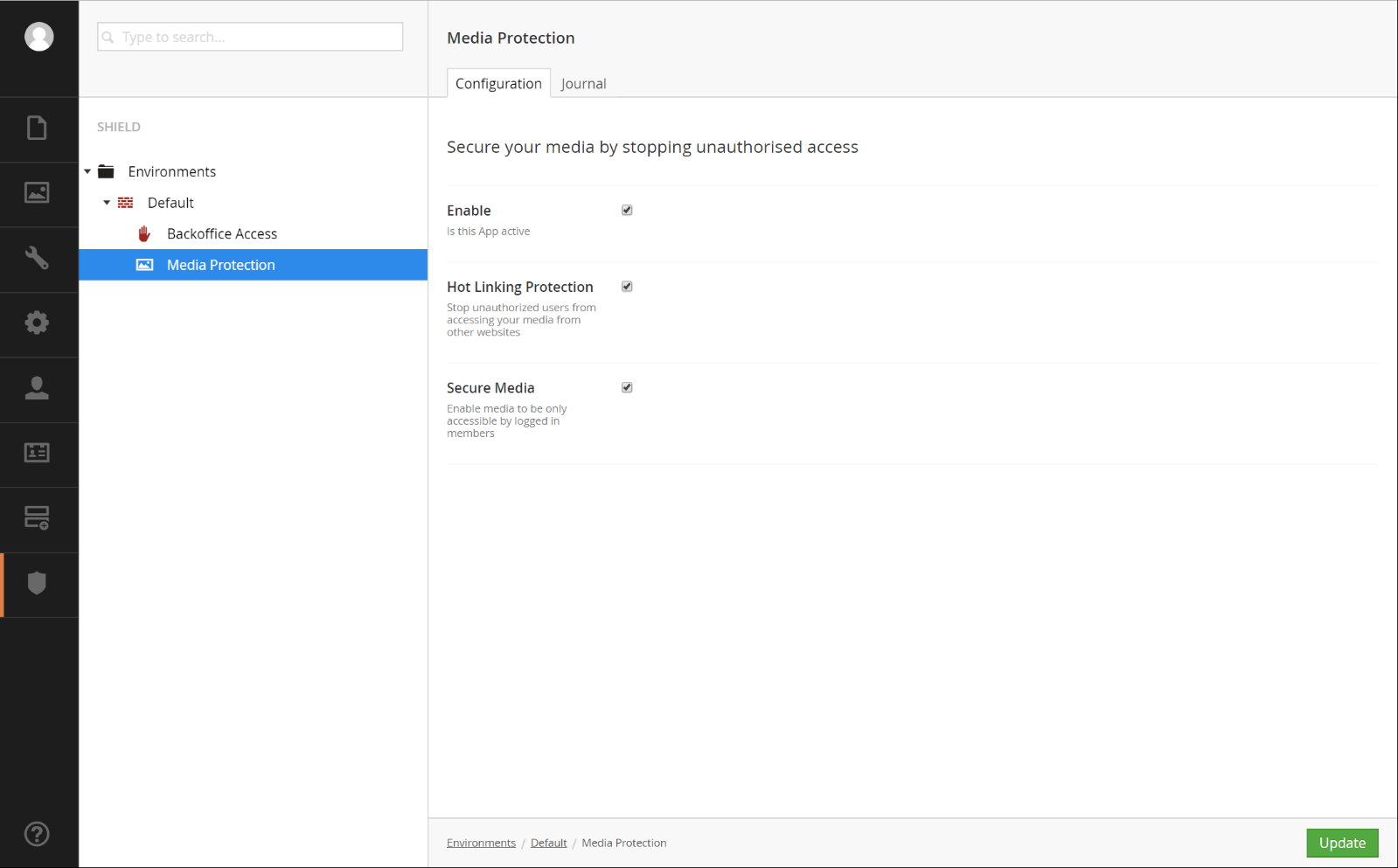
# Our.Shield.MediaProtection

Once Media Protection has been installed, you should find a new node within the tree, or within the app listing on an environment node to access Media Protection’s Configuration and Journal. You should also have 3 new media types created to use, to allow media protection to work as expected.

Media Protection gives you the ability to stop other websites from hotlinking your media assets and allows you to setup media to only be viewed by authenticated users.

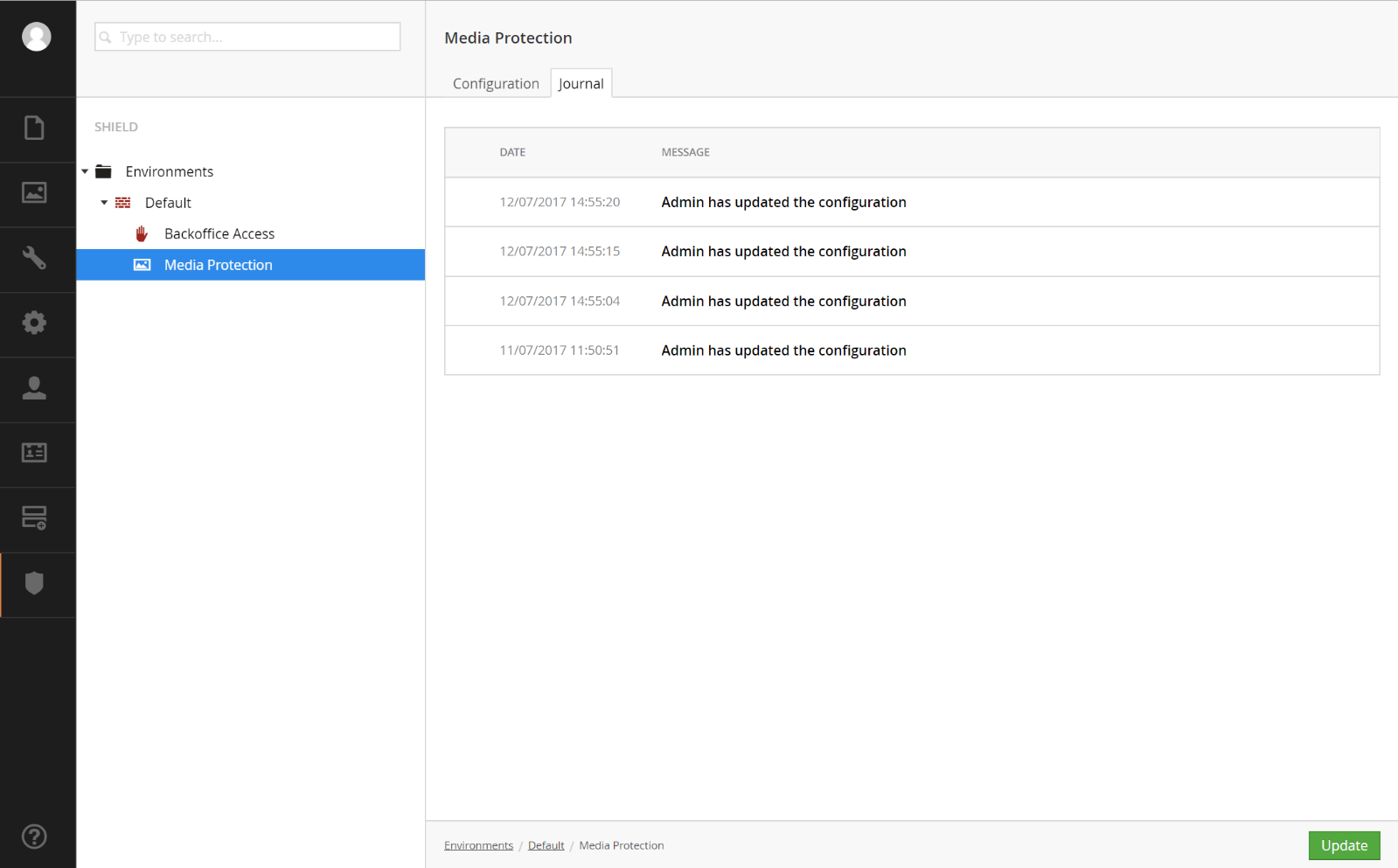
## Configuration

The configuration gives you the ability to enable/disable the shield app and allows you to enable/disable hot linking protection and or secure media.



## Journal

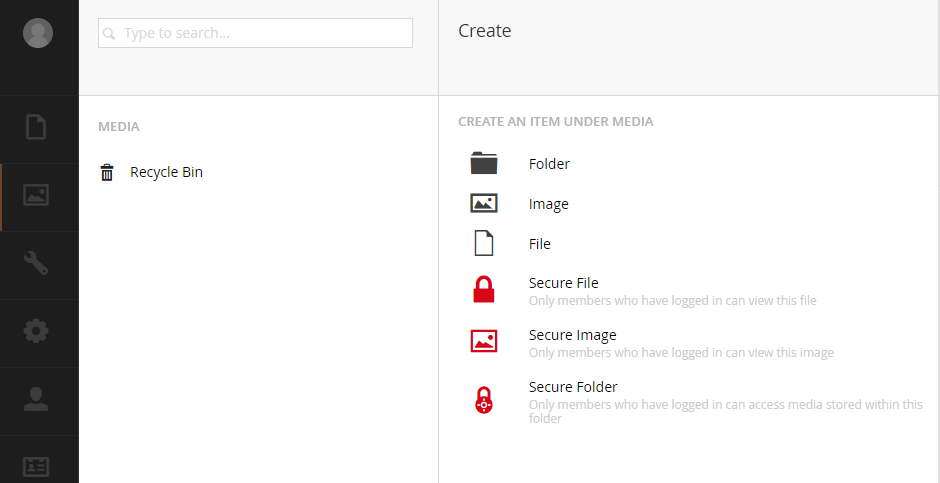
As per the other shield apps’ Journal tab, Media Protection journal only displays the journals for this app and shows the create date of the journal item, and a message as to why the journal item was created.



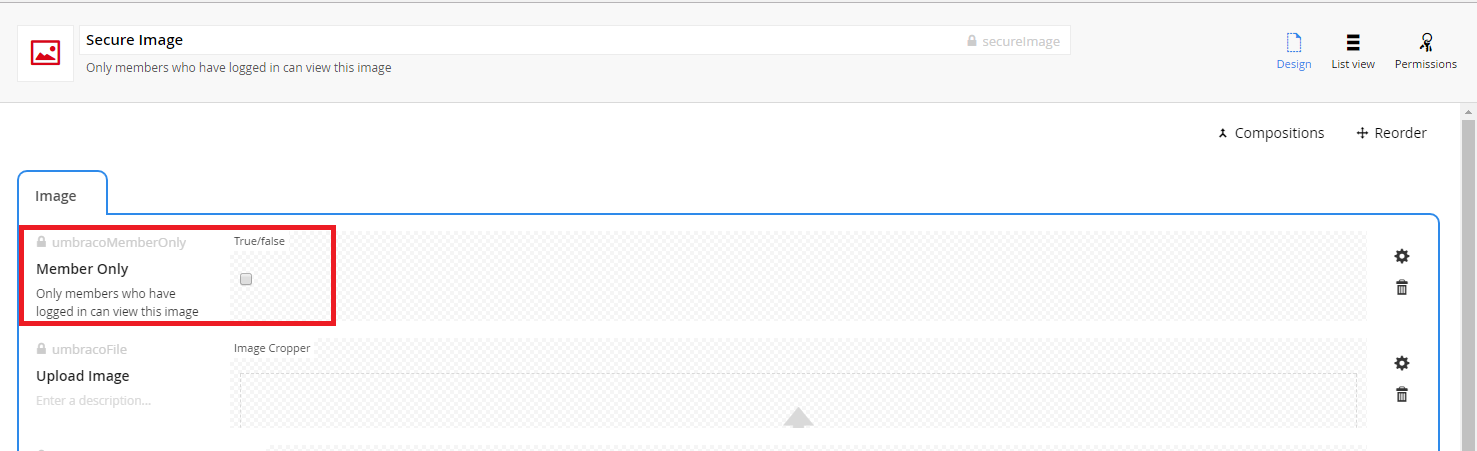
## Media Types

Once Media Protection has been installed, you should have 3 new media types to use:

1. Secure File
2. Secure Image
3. Secure Folder



These 3 new media types are used in conjunction with the Configuration’s “Secure Media” option. You’re able to create more secure media types by creating a new media type and having a property with a special alias of “umbracoMemberOnly” as type “True/False”.



## Hot Linking Protection

Enabling the Hot Linking Protection configuration option, stops others from referencing your media items from their site as a direct resource as opposed to hosting the media item from their site. By doing this, it reduces unwanted traffic coming to your site, which is using up the website hosted machine’s resources.

## Secure Media

To enable the Secure Media to work as expected, you’ll need to create some new media items using one of the above mentioned new media types (or your custom secure media type(s) if you created any). Once the media items have been created, and the “Member Only” tickbox is checked, when the configuration’s Secure Media option is enable, only authenticated users can view the media item where the “Member Only” tickbox is checked.

Disabling Secure Media configuration option will allow access to the media items regardless of whether or not the “Member Only” tickbox on a media item is checked.

If you create a Secure Folder media item, and place all your media items in this secure folder, you’ll only need to check the “Member Only” tickbox on the Secure Folder item. Media Protection will look at the media item’s ancestors (parent nodes), and if an ancestor has the “Members Only” tickbox checked, then all its children are as well. For example, if you had the following media setup:

-Secure Folder

---Secure Image

---Image

---Image

And on the Secure Folder, you have the “Member Only” tickbox checked, then all the children, (the x1 Secure Image & the x2 Image) will only be accessible by authenticated users. The x1 Secure Image item itself doesn’t need the “Member Only” tickbox checked.

# Extending Shield with your own app

Within Visual Studio (or something similar) you’ll need to do the following:

1. Install UmbracoCMS & Our.Shield.Core into your project via nuget

2. Create a class which will be the configuration for your app; the configuration is where you allow the app to be enabled/disabled, allow the end user to edit the configuration, to work the way they desire within the parameters of which your app offers.  
  
So Create a class inheriting from **Our.Shield.Core.Models.Configuration**, you may want to decorate the class with Json attributes as this will be serialized/deserialised to and from the view and the database:   
  
Using Media Protection as an example  
  
[JsonObject(MemberSerialization.OptIn)]  
public class MediaProtectionConfiguration: Configuration  
{   
 [JsonProperty("enableHotLinkingProtection")]  
 public bool EnableHotLinkingProtection { get; set; }  
  
 [JsonProperty("enableMemberOnlyMedia")]  
 public bool EnableMembersOnlyMedia { get; set; }  
}

3. You’ll need To create a class that will be your app, which uses your configuration created in the previous step.  
  
The new class will need to inherit from **Our.Shield.Core.Models.App** passing your configuration as a generic; using media protection as an example:  
  
public class MediaProtectionApp : App<MediaProtectionConfiguration>  
{  
 public override string Id => "MediaProtection"  
  
 public override string Name => "Media Protection";  
  
 public override string Description => "Secure your media by stopping unauthorised access";  
  
 public override string Icon => "icon-picture red";  
  
 public override IConfiguration DefaultConfiguration  
 {  
 get  
 {  
 return new MediaProtectionConfiguration  
 {  
 EnableHotLinkingProtection = true,  
 EnableMembersOnlyMedia = true  
 }  
 }  
 }  
  
 public override bool Execute(IJob job, IConfiguration c)  
 {  
 //We’ll come back to this in a later step  
 return true;  
 }  
}

4. Next is to start to get something to display on the page when someone accesses the app in the backoffice.

First, you’ll need to add an attribute to your app class:

[AppEditor("/App\_Plugins/Shield.MediaProtection/Views/MediaProtection.html")]  
public class MediaProtectionApp : App<MediaProtectionConfiguration>  
{  
 ...  
}

secondly, create a html file at the specified location. Leave the html file blank for now.  
  
Now that there’s a class inheriting from **Our.Shield.Core.Models.App** and defining the view for our configuration. If you were to ***Compile*** and ***Run*** your solution, you should notice within the Shield section of Umbraco, your newly created Shield App listed within the Tree, and upon clicking it, displaying your blank html file. Well…

not blank, you should notice that your app view already has 2 tabs, Configuration and Journal. On the Configuration tab, you should see the description of your app, and an enable tickbox option; and on the Journal tab, you should notice the Journal listing, which is handled out-of-the-box, with pagination once there’s more than 50 journal items (as long as you write to it in code! Out-of-the-box, Shield’s framework will add a journal item whenever the configuration is saved).

Let’s populate our html file with some code, using Media Protection as an example:

<div ng-controller="Shield.Editors.MediaProtection.Edit as vm">  
 <div class="umb-el-wrap control-group umb-control-group">  
 <label for="hotlinking" class="control-label">  
 <span>Hot Linking Protection</span>  
 <small>  
 Stop unauthorized users from accessing your media from other websites  
 </small>  
 </label>  
 <div class="controls">  
 <input type="checkbox" id="hotlinking"

ng-model="vm.configuration.enableHotLinkingProtection" />  
 </div>  
 </div>  
  
 <div class="umb-el-wrap control-group umb-control-group">

<label for="securemedia" class="control-label">

<span>Secure Media</span>

<small>

Enable media to be only accessible by logged in members

</small>

</label>

<div class="controls">

<input type="checkbox" id="securemedia"

ng-model=" vm.configuration.enableMemberOnlyMedia" />

</div>

</div>  
</div>

***Note:*** *Your configuration view will only be displayed by Shield’s framework, when the app is enabled. While disabled, only the Enable**option is displayed!*

Thirdly, we’ll also need to create an angular controller to handle anything specific to your Shield App, this includes but not limited to, any validation on your configuration properties.

So create a new js file within you solution and populate it with:

Using Media Protection as an example

angular.module('umbraco').controller('Shield.Editors.MediaProtection.Edit',  
 ['$scope', function ($scope) {  
 var vm = this;  
 angular.extend(vm, {  
 configuration: $scope.$parent.configuration  
 });  
 }]  
);

***Note: $scope.$parent.configuration*** *will be a serialised version of the configuration created in step 1.*

Finally, you’ll need to create a package.manifest for Umbraco to load your js file containing your angular controller

**Compiling** and **Running** your Shield App now, you should notice you have a fully functional app from a UI perspective. You should have the ability to enable / disable your app, change any other configuration, and save your configuration.

5. Time to return to the Execute method created in step 3.