

# 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/>

```
PM> Install-Package Our.Shield.Core -Version 1.0.3
```

And the second part is the Shield apps, which provide 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 and restrict access to the backoffice access URL.

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

```
PM> Install-Package Our.Shield.BackofficeAccess -Version 1.0.3
```

- **Media Protection**

Disable [Hotlinking](#) and to secure your media to only be accessed by authenticated members.

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

```
PM> Install-Package Our.Shield.MediaProtection -Version 1.0.3
```

- **Frontend Access**

Gives you the ability to lock down the frontend to only be accessible by authenticated Umbraco Users and/or restrict via IP address(es)

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

```
PM> Install-Package Our.Shield.FrontendAccess -Version 1.0.3
```

- **Elmah**

Adds the popular error logging library elmah to your site, with the ability to add security restrictions to ~/elmah.axd

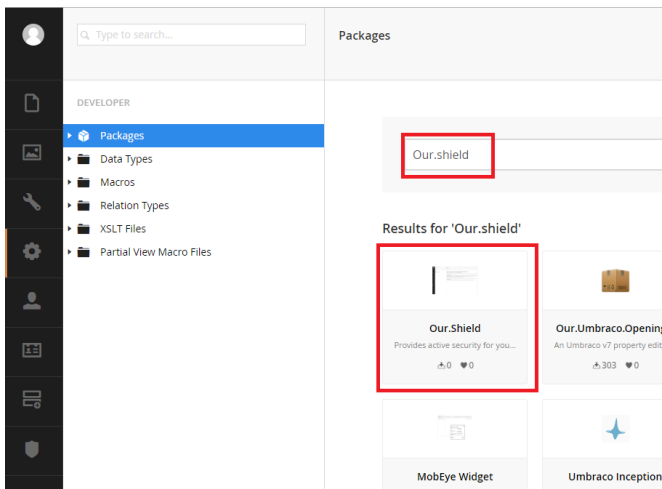
<https://www.nuget.org/packages/Our.Shield.Elmah>

## Installing via Umbraco Package Manager

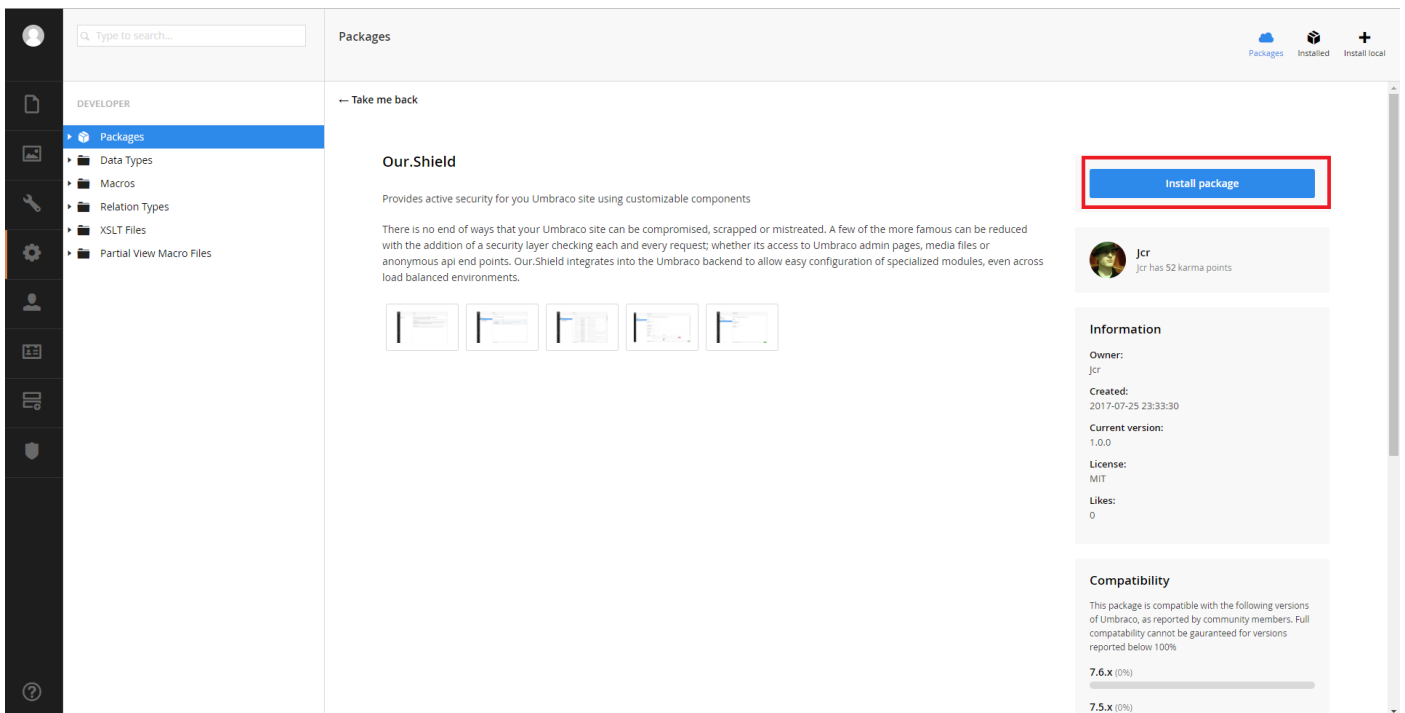
<https://our.umbraco.org/projects/backoffice-extensions/ourshield/>

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

First, navigate to the developer section of Umbraco, click on the packages node and search for Shield



Next, Click on the package, and then the install button

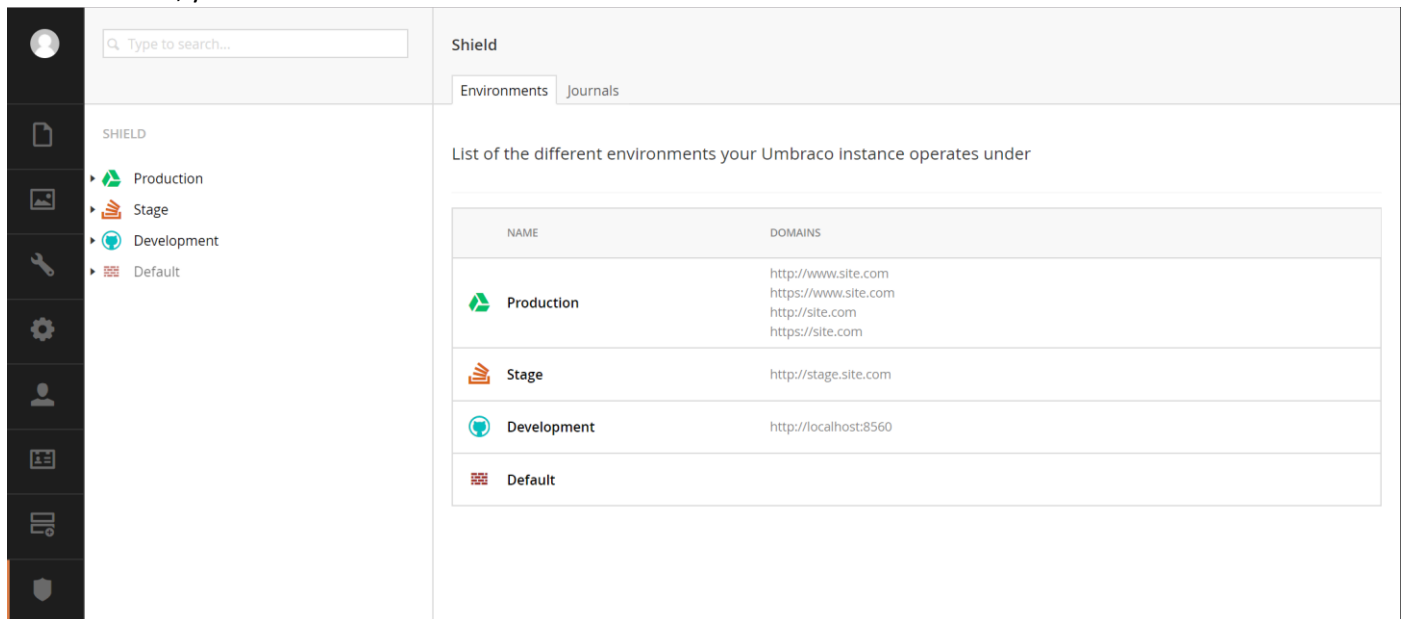


Afterwards, Shield should be installed





## Shield

Shield is the framework for the apps that can be installed to provide the active security. It contains the custom section to be displayed in Umbraco and does the 'heavy' lifting for the installed app(s).

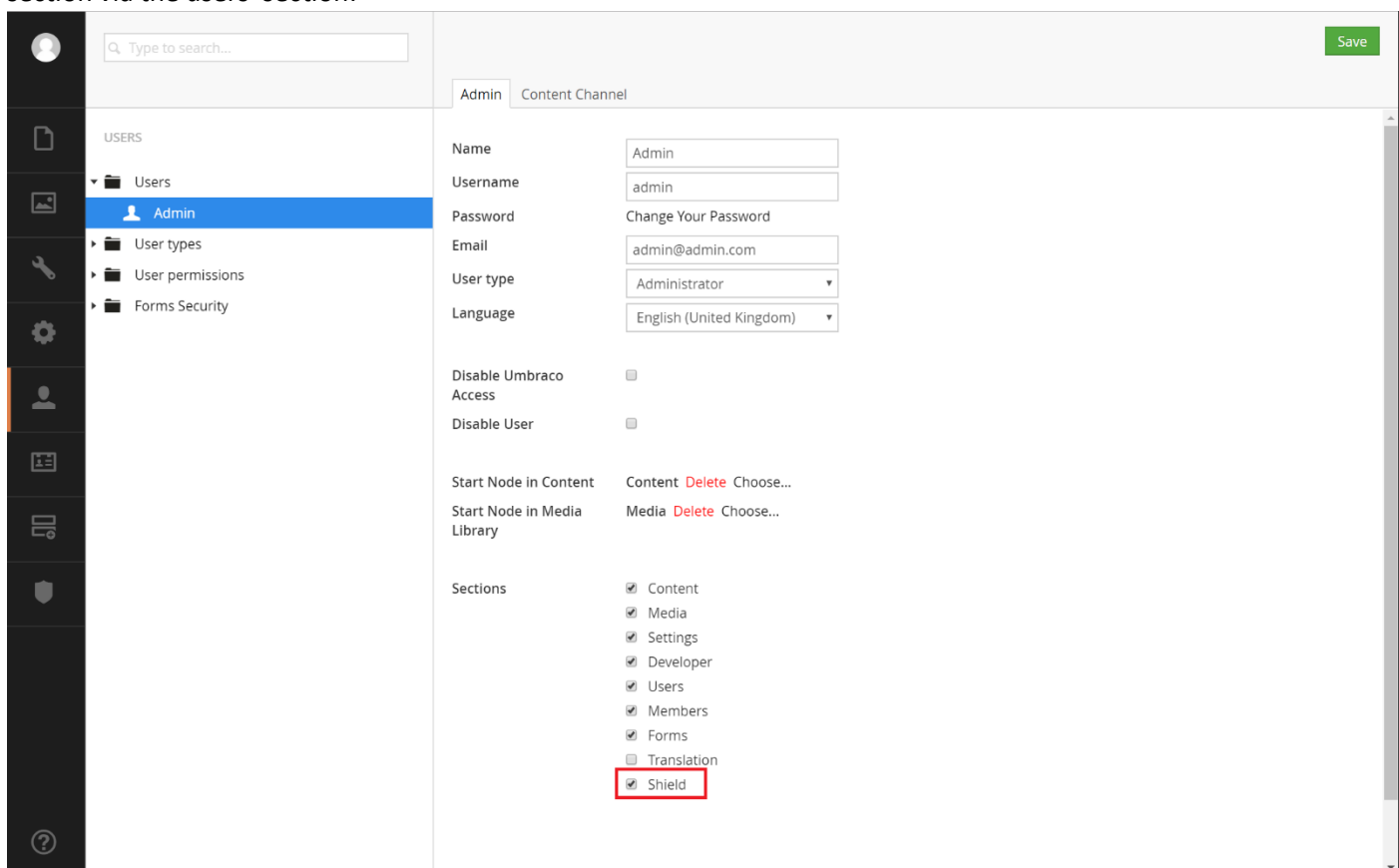
Once installed, you should see a new custom section within the backoffice of Umbraco.



The screenshot shows the Umbraco backoffice interface. On the left is a sidebar with icons for various sections. The main content area is titled 'Shield' and has two tabs: 'Environments' (selected) and 'Journals'. Below the tabs, there is a heading 'List of the different environments your Umbraco Instance operates under'. A table follows, listing environments and their domains.

NAME	DOMAINS
 Production	http://www.site.com https://www.site.com http://site.com https://site.com
 Stage	http://stage.site.com
 Development	http://localhost:8560
 Default	

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:



The screenshot shows the 'Admin' user profile in the Umbraco backoffice. The 'Admin' user is selected in the sidebar. The main content area shows the user's details and permissions. The 'Sections' section is expanded, and the 'Shield' checkbox is checked, indicating that the user has access to the Shield section.

**Admin** | Content Channel

**Name:** Admin

**Username:** admin

**Password:** Change Your Password

**Email:** admin@admin.com

**User type:** Administrator

**Language:** English (United Kingdom)

**Disable Umbraco Access:** ☐

**Disable User:** ☐

**Start Node in Content:** Content [Delete](#) [Choose...](#)

**Start Node in Media Library:** Media [Delete](#) [Choose...](#)

**Sections:**

- ☒ Content
- ☒ Media
- ☒ Settings
- ☒ Developer
- ☒ Users
- ☒ Members
- ☒ Forms
- ☐ Translation
- ☒ **Shield**

## Environments Dashboard

Initially, a 'Default' environment is created, which acts as a catch all environment and responds to all requests. Any app enabled and configured in the 'Default' environment will respond and process any request (this can be frontend webpages, backend, media or Web API requests) if none of the previous environments responded to a request because they don't match the request's domain. As you create new environments with their own domains, any requests on those domains will be handled by the apps enabled and configured within that environment.

This allows different configuration of apps for your different environments; for example, Hot Linking protection only on your Production environment and Frontend Access restrictions on your Staging environment.

SHIELD

Production

Stage

Development

Default

Shield

Environments Journals

List of the different environments your Umbraco instance operates under

NAME	DOMAINS
<div>Production</div>	<div>http://www.site.com</div> <div>https://www.site.com</div> <div>http://site.com</div> <div>https://site.com</div>
<div>Stage</div>	<div>http://stage.site.com</div>
<div>Development</div>	<div>http://localhost:8560</div>
<div>Default</div>	

## Journals Dashboard

The Journal tab will display all journal items (logs) that have been created by the different environment(s) and 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 this Journal item
- The app that created the Journal item
- A message of why the Journal item was created

SHIELD

Production

Stage

Development

Default

Shield

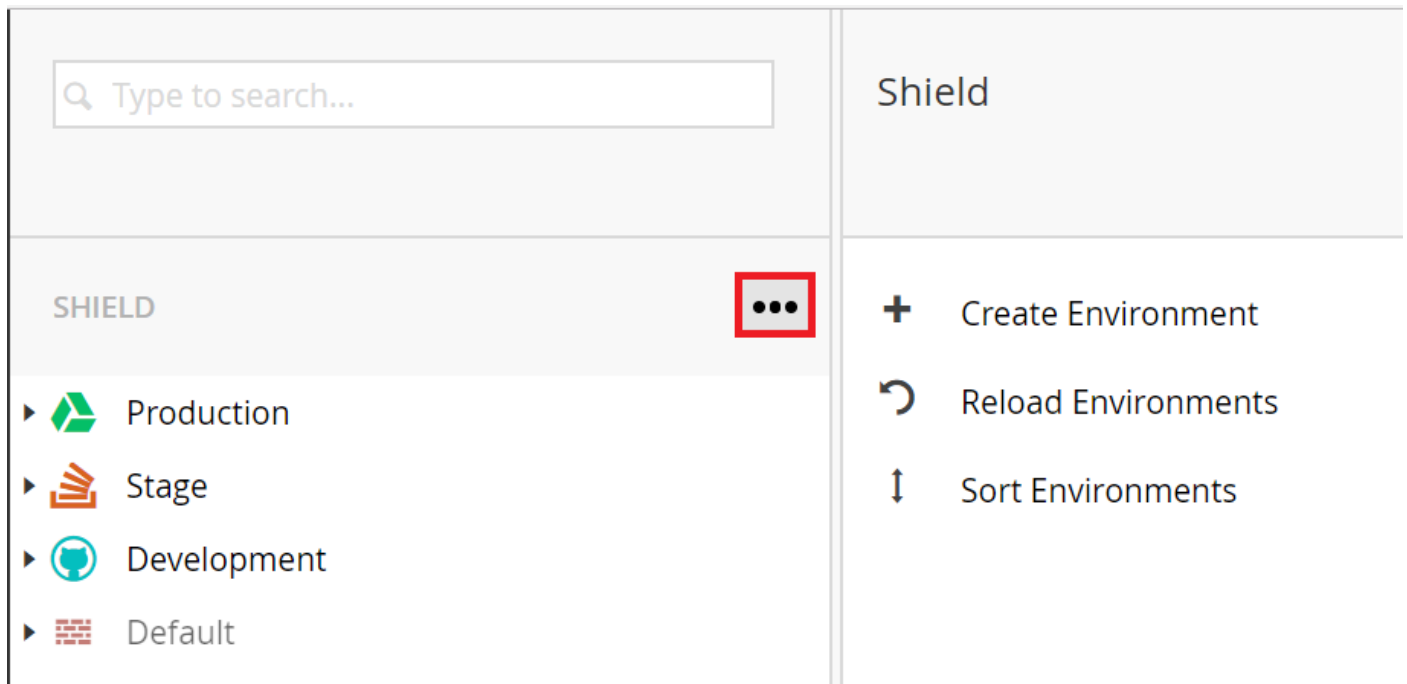
Environments Journals

DATE	ENVIRONMENT	APP	MESSAGE
31/08/2017 22:19:30	Stage	Media Protection	admin has updated the configuration
31/08/2017 22:19:10	Stage	Frontend Access	admin has updated the configuration
31/08/2017 22:18:54	Stage	Backoffice Access	admin has updated the configuration
31/08/2017 22:18:26	Production	Media Protection	admin has updated the configuration
31/08/2017 22:18:09	Production	Backoffice Access	admin has updated the configuration
31/08/2017 19:26:49	Development	Backoffice Access	admin has updated the configuration
31/08/2017 19:26:44	Development	Backoffice Access	admin has updated the configuration
31/08/2017 17:52:38	Development	Backoffice Access	admin has updated the configuration
31/08/2017 17:52:21	Development	Backoffice Access	admin has updated the configuration
31/08/2017 17:37:41	Development	Backoffice Access	admin has updated the configuration
31/08/2017 17:34:36	Development	Media Protection	admin has updated the configuration

## Tree

The tree will show a listing of the environments configured, with the desired Icon and name with a visual indication of whether or not the environment is active.

Clicking the three dots to Shield's root node:



Gives you the ability to create, reload, and sort the environments

## Create Environment

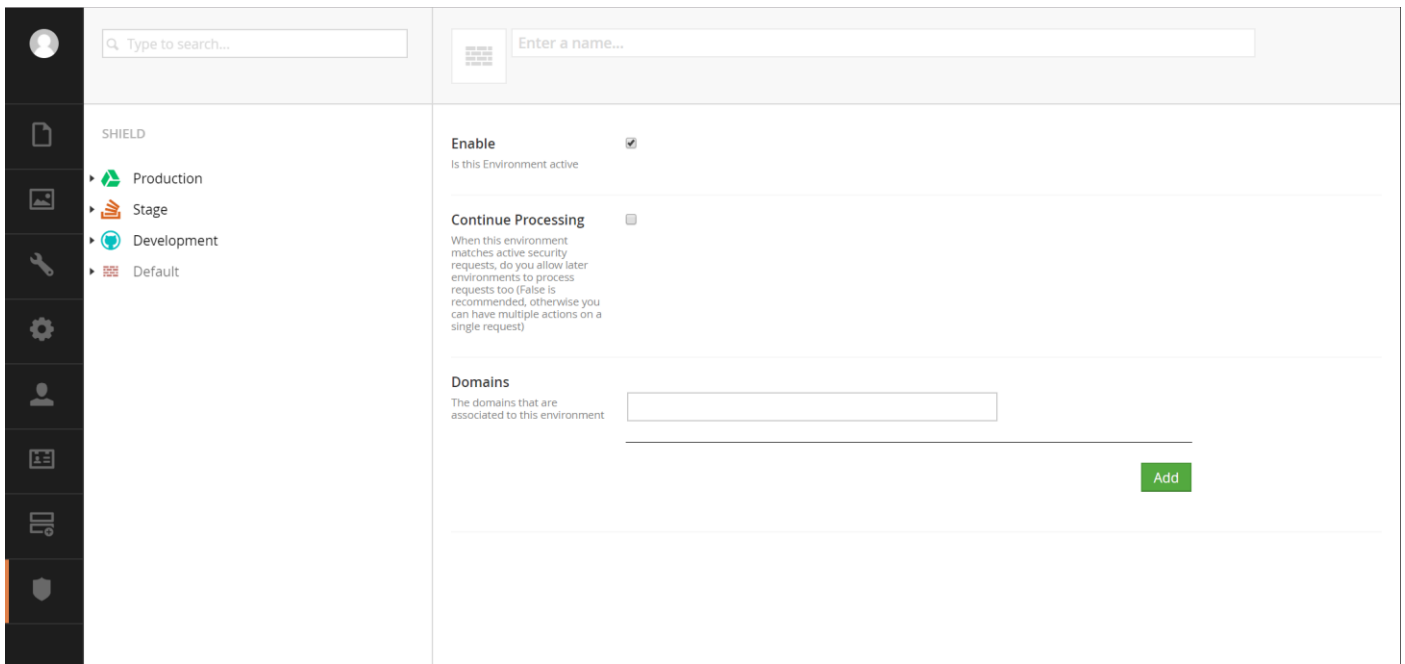
When creating an environment, you'll have the ability to

- Select an **Icon** that identifies visually this environment
- Set an unique **Name** for this environment
- **Enabled** this environment. When disabled all of the apps within the environment are disabled too. This is equivalent of the environment not existing. This can mean that requests that could have been handled by this environment will now be processed by the 'Default' Environment.
- **Continue Processing** allows future environments to process and handle a web request even if this environment has already processed it. This allows the chaining of app configurations across environments. We consider this as advanced behaviour and so suggest to keep this setting as false for simplicity.
- Add a list of **Domains** that define this environment. So for example if your Production environment used [www.mydomain.com](http://www.mydomain.com) and [www.myotherdomain.com](http://www.myotherdomain.com), then for a production environment you would type <http://www.mydomain.com> and <http://www.myotherdomain.com>, then whenever Shield processes an active request it could identify those that belong to your Production environment because they match these two domains.

All web requests have a domain, the domain of the request is compared to the list of domains an environment has, if they match then each of the apps for that domain are processed.

If **Continue Processing** is true, then other environments are checked for matching domains also and if they match, then the apps associated with that domain are processed too. And then finally the 'Default' environment is processed.

When **Continue Processing** is false, no further environments are processed including 'Default'.



## Sort Environments

Once you have multiple environments, you should order them with the Production environment first, and the development environment last (before default). An example could be:

- Production
- Preview
- Staging
- QA
- Development

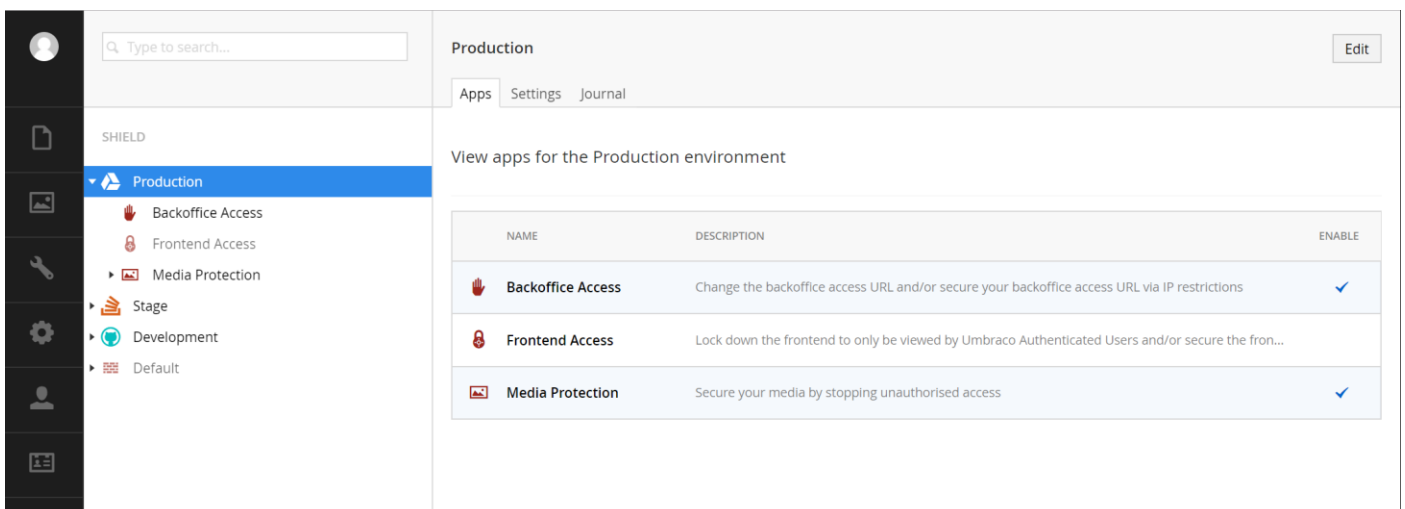
The reason for Production being first, is that this will, ever so slightly, be processed first and will speed up any Live requests – which normally is more important, but it is all very marginal.

## Environment Node

An Environment will display all installed apps, the ability to edit an environment and view Journal entries. To edit an environment, there's an 'Edit' button to the right of the environment's name. The Edit view is the same as the create environment view, giving you the full ability to modify the environment as needed.

## Apps

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 corresponding app's configuration.



## Settings

The Settings tab is very similar to creating/editing an environment, the difference being, on the settings tab, you don't have the ability to change the icon or edit the name.

The screenshot shows the 'Settings' tab for the 'Production' environment. The left sidebar contains a search bar and a list of environments: SHIELD, Production (selected), Backoffice Access, Frontend Access, Media Protection, Stage, Development, and Default. The main content area has tabs for 'Apps', 'Settings', and 'Journal'. The 'Settings' tab is active, showing options to 'Enable' the environment (checked), 'Continue Processing' (unchecked), and a list of 'Domains' with input fields and 'Remove' buttons.

**Production** Edit

Apps Settings **Journal**

**Enable** ☒  
Is this Environment active

**Continue Processing** ☐  
When this environment matches active security requests, do you allow later environments to process requests too (False is recommended, otherwise you can have multiple actions on a single request)

**Domains**  
The domains that are associated to this environment

<input type="text" value="http://www.site.com"/>	<span>Remove</span>
<input type="text" value="https://www.site.com"/>	<span>Remove</span>
<input type="text" value="http://site.com"/>	<span>Remove</span>
<input type="text" value="https://site.com"/>	<span>Remove</span>

## Journal

Similar to the Journal Dashboard, this will display the Journal items only for the selected environment. The difference being, the environment column is not included and only shows journal entries relevant to the selected environment.

The screenshot shows the 'Journal' tab for the 'Production' environment. The left sidebar is identical to the previous screenshot. The main content area has tabs for 'Apps', 'Settings', and 'Journal'. The 'Journal' tab is active, displaying a table of log entries with columns for DATE, APP, and MESSAGE.

**Production** Edit

Apps Settings **Journal**

DATE	APP	MESSAGE
31/08/2017 22:18:26	<b>Media Protection</b>	admin has updated the configuration
31/08/2017 22:18:09	<b>Backoffice Access</b>	admin has updated the configuration

## Backoffice Access

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 if desired.

### Configuration

- Enable or disable this app. When disabled the URL will return to the predefined default, which is “/umbraco”.
- The backoffice access URL you wish to use, to access the admin area of Umbraco. This can be any valid combination of letters or numbers, non-case sensitive. You are not allowed white space, symbols or special characters.
- Whether the frontend is accessible by all IP addresses or to specific IP Addresses
- Whether to play dead, redirect or rewrite the request to another location
- The URL to redirect or rewrite the request to.

The screenshot shows the Umbraco administration interface for the 'Backoffice Access' app. On the left is a sidebar with a search bar and a list of apps under 'Development', including 'Backoffice Access' (which is selected), 'Elmah', 'Frontend Access', 'Google Safe Browsing', 'Media Protection', 'Scraper Defense', and 'Site Maintenance'. The main panel is titled 'Backoffice Access' and has two tabs: 'Configuration' and 'Journal'. The 'Configuration' tab is active, showing options to 'Enable' the app (checked), set the 'Backend Office Access URL' to 'admin', and configure 'IP Addresses Access'. Under 'IP Addresses Access', there are two radio buttons: 'Open to all IP addresses' (selected) and 'No access for all IP addresses'. Below this is a table of IP addresses with columns 'IP Address' and 'Description'. The table contains two entries: '127.0.0.1' with description 'localhost' and '127.0.0.2 - 127.0.0.10' with description 'localhost2'. Each entry has 'Edit' and 'Remove' buttons. An 'Add' button is at the bottom of the table. At the bottom of the configuration panel, there is an 'Unauthorized' section with a dropdown set to 'Rewrite', a 'Url' dropdown, and a text input field containing '/403.html'. An 'Update' button is in the bottom right corner.

### Journal

Similar to the Journal Dashboard, this will only show the journal entries for the selected app & environment. The list will show warnings, messages and errors that have occurred within the app. This includes all unauthorised attempts to gain access to the backoffice access URL.

## Upgrading Umbraco with Backoffice Access

To upgrade Umbraco while Backoffice Access is enabled or disabled, ensure within the website's web.config file the 'umbracoPath' and 'umbracoReservedPaths' app settings are 'umbraco' respectively:

```
<appSettings>
  <add key="umbracoConfigurationStatus" value="7.5.14" />
  <add key="umbracoReservedUrls" value="~/config/splashes/booting.aspx,~/install/default.aspx,~/config/splashes/noNodes.aspx,~/VSEnterpriseHelper.axd" />
  <add key="umbracoReservedPaths" value="~/umbraco,~/install/" />
  <add key="umbracoPath" value="~/umbraco" />
  <add key="umbracoUseDirectoryUrls" value="true" />
  <add key="umbracoUseDirectoryUrls" value="true" />
  <add key="umbracoTimeoutInMinutes" value="60" />
</appSettings>
```

As well as the location element (if set, and ensure there is only one!):



```
</runtime>
<location path="umbraco">
  <system.webServer>
    <urlCompression doStaticCompression="false" doDynamicCompression="false" dynamicCompressionBeforeCache="false" />
  </system.webServer>
</location>
<location path="App_Plugins">
  <system.webServer>
    <urlCompression doStaticCompression="false" doDynamicCompression="false" dynamicCompressionBeforeCache="false" />
  </system.webServer>
</location>
```

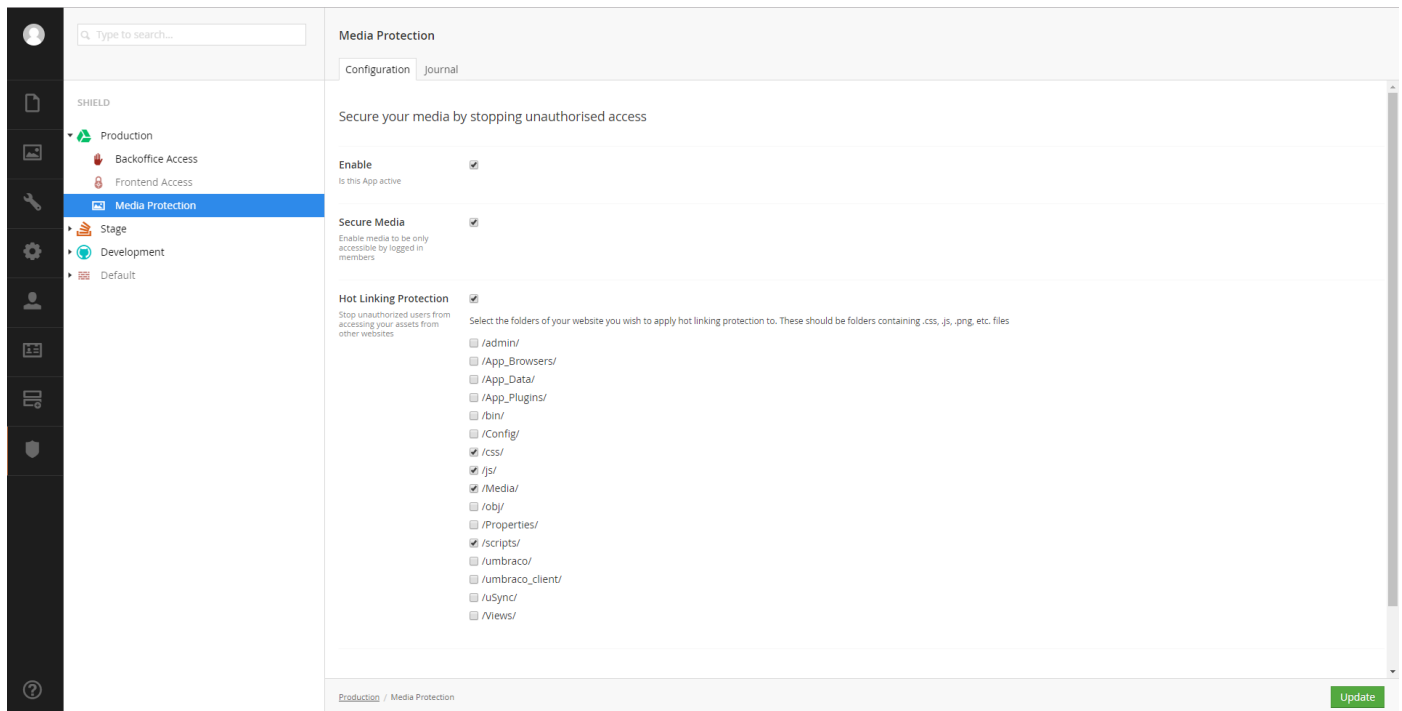
This is because, as part of Backoffice Access functionality, it will set these to whatever your preferred access URL is. You should then be able to upgrade Umbraco the normal way via the installer/upgrader, using the URL '/umbraco'. Once the upgrade process has been completed, you'll find '/umbraco' URL will no longer be accessible again, and will continue to work from your preferred access URL. You don't need to reset these web.config values back to your preferred access URL, as Backoffice Access will handle this for you on the next app pool restart.

## Media Protection

Media Protection gives you the ability to stop other websites from hot linking your media assets and allows you to assign media to only be viewed by authenticated members.

### Configuration

- Enable or disable this app. When disabled there will be no active security on your website's assets.
- When Secure Media is enabled, any Secure Folder, Image or File items that they, themselves have been specifically set to be Members only are restricted to your front-end users that have logged in.
- When Hot linking protection is enabled, it'll show all the folders at the root of your website, you'll need to select the folder(s) you desire to add hot linking protection to. Ideally, you should select the folder(s) that contain your website's assets. i.e. the media folder, folder(s) that contain .css, .js, .png, etc. files



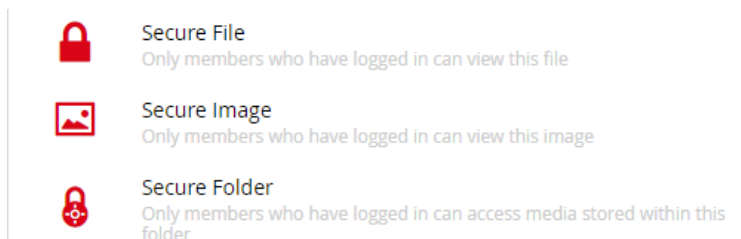
### Journal

As per the other Journal listings, it displays journals that have been logged for this environment & app. The list will show warnings, messages and errors that have occurred within the app. This includes all unauthorised attempts to hot link your website's assets.

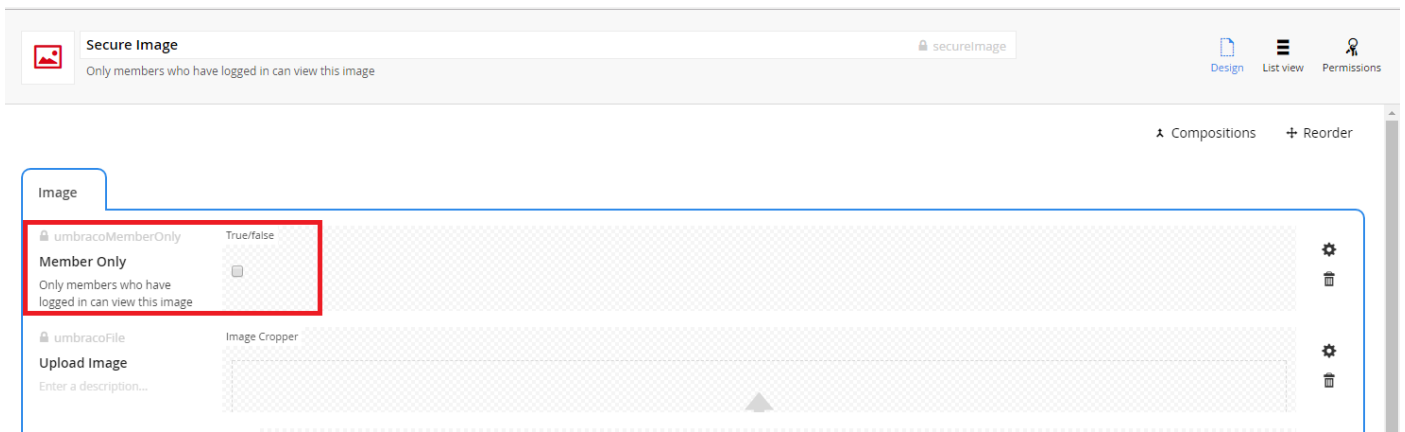
### Media Types

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".



## 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 for said media items, as well as the configuration's Secure Media option is enable, only authenticated members can view the media items 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.

## Frontend Access

Frontend Access gives you the ability to lock down the frontend of your website to either those authenticated Umbraco backend Users and/or IP Address restrictions. Ideally this app should be disabled on your production website (or the default environment), and enabled on your other environments – if you have multiple environments setup.

### Configuration

- The ability to enable/disable this app. When disabled this app doesn't limit access to the frontend in any way.
- Whether the frontend of your website is accessible by authenticated Umbraco Users
- Whether the frontend is accessible by all IP addresses or to specific IP Addresses
- Whether to play dead, redirect or rewrite the request to another location
- The URL to redirect or rewrite the request to.

The screenshot shows the Umbraco administration interface for the 'Frontend Access' app. On the left is a sidebar with a search bar and a list of apps under a 'Shield' icon: Development, Backoffice Access, Elmah, Frontend Access (highlighted), Google Safe Browsing, Media Protection, Scraper Defense, Site Maintenance, and Default. The main panel is titled 'Frontend Access' and has two tabs: 'Configuration' and 'Journal'. The 'Configuration' tab is active, showing the following settings:

- Restrict access to the frontend to Umbraco Authenticated Users and/or via IP Address restrictions**
- Enable**: A checkbox labeled 'Is this App active' is checked.
- Allow Authenticated Umbraco Users**: A checkbox is checked, with a description: 'Whether or not the Frontend is accessible by users who have authenticated as an Umbraco User'.
- IP Addresses Access**: Two radio buttons are present: 'Open to all IP addresses' (selected) and 'No access for all IP addresses'. Below, it says 'Except for these IP Addresses:' and shows a table:

IP Address	Description	
127.0.0.1	localhost	<button>Edit</button> <button>Remove</button>
127.0.0.2 - 127.0.0.10	localhost range	<button>Edit</button> <button>Remove</button>

Add
- Unauthorized**: A section with three fields: 'Rewrite' (a dropdown menu), 'Url' (a dropdown menu), and a text input field containing '/403.html'.

At the bottom right of the configuration panel is a green 'Update' button. The breadcrumb at the bottom reads 'Development / Frontend Access'.

### Journal

Lists all unauthorised attempts to access the frontend of your website, as well as saves and updates of the configuration.

# Elmah

Elmah adds the popular error logging library ELMAH to umbraco and allows you to restrict access to ~/elmah.axd

## Reporting

An access point to elmah's error log within the backoffice of umbraco.

Type to search...

Shield

Development

Backoffice Access

Elmah

Frontend Access

Google Safe Browsing

Media Protection

Scrapper Defense

Site Maintenance

Default

Elmah

Reporting

Configuration

Journal

Host	Code	Type	Error	Date	Time
JCR-SURFACE	0	Elmah.TestException	This is a test exception that can be safely ignored.	08/01/2018	21:32
JCR-SURFACE	0	Elmah.TestException	This is a test exception that can be safely ignored.	08/01/2018	21:32
JCR-SURFACE	0	Elmah.TestException	This is a test exception that can be safely ignored.	08/01/2018	21:32
JCR-SURFACE	0	Elmah.TestException	This is a test exception that can be safely ignored.	08/01/2018	21:32
JCR-SURFACE	0	Elmah.TestException	This is a test exception that can be safely ignored.	08/01/2018	21:31

Development / Elmah

Update

Clicking on a log will open that log and show more details about the error.

Type to search...

Shield

Development

Backoffice Access

Elmah

Frontend Access

Google Safe Browsing

Media Protection

Scrapper Defense

Site Maintenance

Default

Elmah

Reporting

Configuration

Journal

Back to listing

Host	JCR-SURFACE
Code	0
Type	Elmah.TestException
Error	This is a test exception that can be safely ignored.
Date	2018-01-08
Time	21:48

StackTrace

Elmah.TestException: This is a test exception that can be safely ignored. at Elmah.ErrorLogPageFactory.FindHandler(String name) at Elmah.ErrorLogPageFactory.GetHandler(HttpContext context, String requestType, String url, String pathTranslated) at System.Web.HttpApplication.MaterializeHandlerExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute() at System.Web.HttpApplication.ExecuteStepImpl(IExecutionStep step) at System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously)

Development / Elmah

Update

## Configuration

- The ability to enable/disable this app. When disabled this app doesn't limit access to ~/elmah.axd in any way.
- Whether ~/elmah.axd is accessible by authenticated Umbraco Users
- Whether ~/elmah.axd is accessible by all IP addresses or to specific IP Addresses
- Whether to play dead, redirect or rewrite the request to another location
- The URL to redirect or rewrite the request to.

The screenshot shows the 'Elmah' configuration page in the Umbraco CMS. The left sidebar contains a 'Shield' menu with options like Development, Backoffice Access, Elmah (selected), Frontend Access, Google Safe Browsing, Media Protection, Scraper Defense, Site Maintenance, and Default. The main content area is titled 'Elmah' and has tabs for 'Reporting', 'Configuration', and 'Journal'. The 'Configuration' tab is active, showing settings for restricting access to ~/elmah.axd. The 'Enable' checkbox is checked. The 'Allow Authenticated Umbraco Users' checkbox is also checked. The 'IP Addresses Access' section shows two radio buttons: 'Open to all IP addresses' (selected) and 'No access for all IP addresses'. Below this, a table lists IP addresses with their descriptions. The 'Unauthorized' section has dropdowns for 'Rewrite' and 'Url', with a text input field for the URL.

IP Address	Description	Edit	Remove
127.0.0.1	localhost		

[Add](#)

**Unauthorized**  
The page to redirect / rewrite the user to, when access is being denied

[Update](#)

## Journal

Lists all unauthorised attempts to access ~/elmah.axd, as well as saves and updates of the configuration.

The screenshot shows the 'Elmah' Journal page in the Umbraco CMS. The left sidebar is the same as in the Configuration page. The main content area is titled 'Elmah' and has tabs for 'Reporting', 'Configuration', and 'Journal'. The 'Journal' tab is active, showing a list of events. The table has columns for 'Date' and 'Message'.

Date	Message
08/01/2018 21:32:21	Admin has updated the configuration
08/01/2018 21:31:59	User with IP Address: ::1; tried to access http://localhost:8560/elmah.axd/test Access was denied
08/01/2018 19:56:33	User with IP Address: ::1; tried to access http://localhost:8560/elmah.axd Access was denied
08/01/2018 19:56:18	User with IP Address: ::1; tried to access http://localhost:8560/elmah.axd/test Access was denied
08/01/2018 19:43:05	Admin has updated the configuration
31/12/2017 17:55:37	Admin has updated the configuration
31/12/2017 17:55:28	Admin has updated the configuration
31/12/2017 17:42:54	Admin has updated the configuration
31/12/2017 17:42:42	Admin has updated the configuration
31/12/2017 17:42:15	Admin has updated the configuration
31/12/2017 17:36:12	Admin has updated the configuration
31/12/2017 17:35:51	Admin has updated the configuration
31/12/2017 17:24:40	Admin has updated the configuration
31/12/2017 17:24:16	Admin has updated the configuration
31/12/2017 17:17:14	Admin has updated the configuration

[Update](#)