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

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

- **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

- **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

- **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

  PM> Install-Package Our.Shield.Elmah

- **Swagger**
  Adds swagger to your site, configured to ignore Umbraco's API's with the ability to adds security restrictions to ~/swagger

  https://www.nuget.org/packages/Our.Shield.Swagger

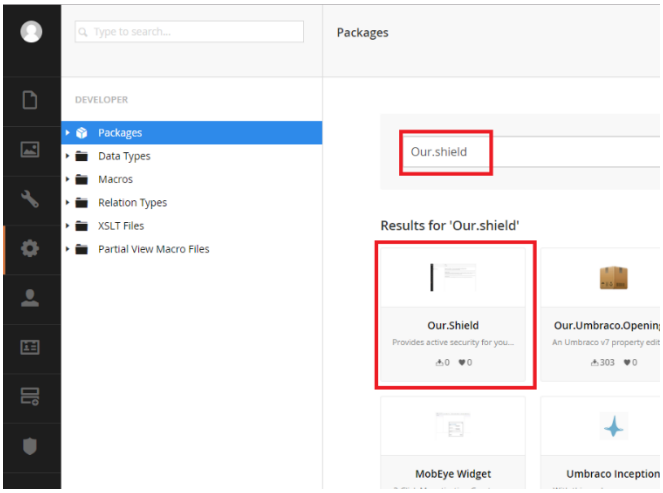
```
PM> Install-Package Our.Shield.Swagger
```

Installing via Umbraco Package Manager

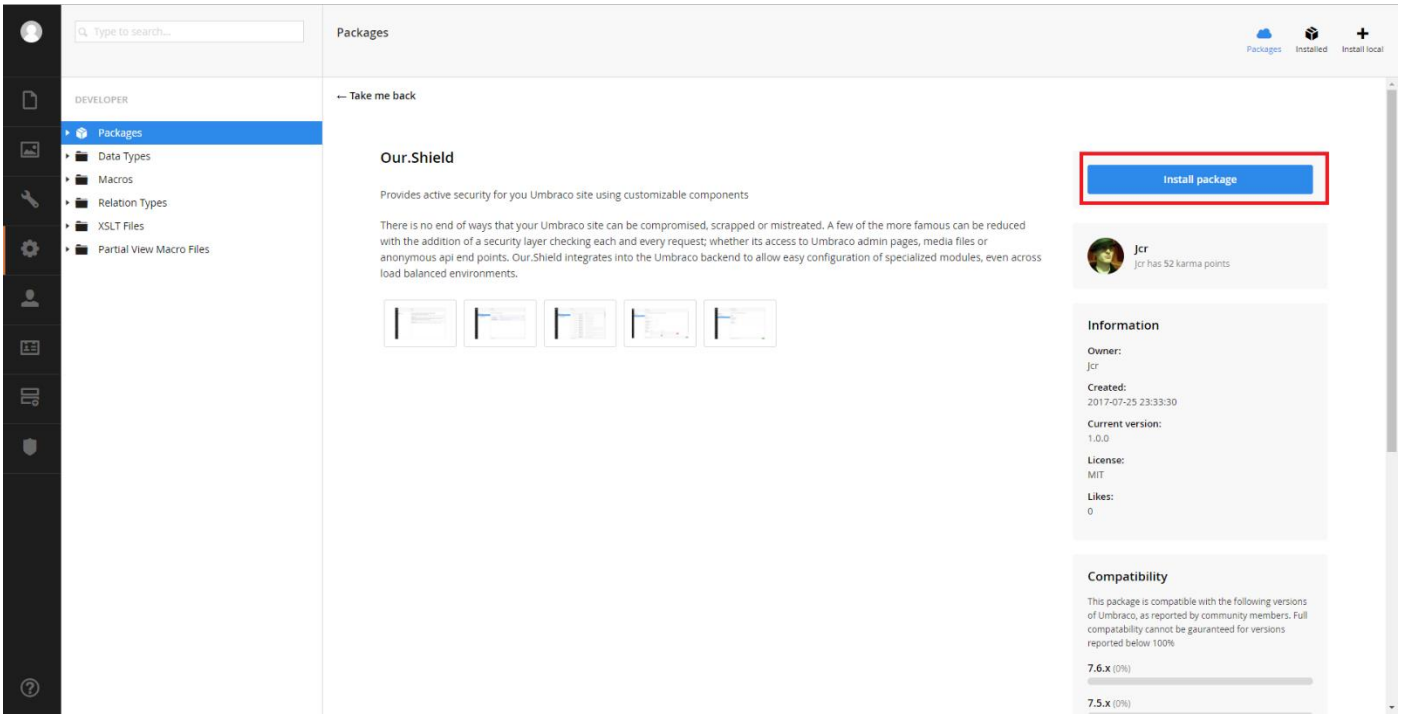
https://our.umbraco.org/projects/backoffice-extensions/ourshield/

This installation contains the Shield framework, and all available Shield apps apart from Elmah app.

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

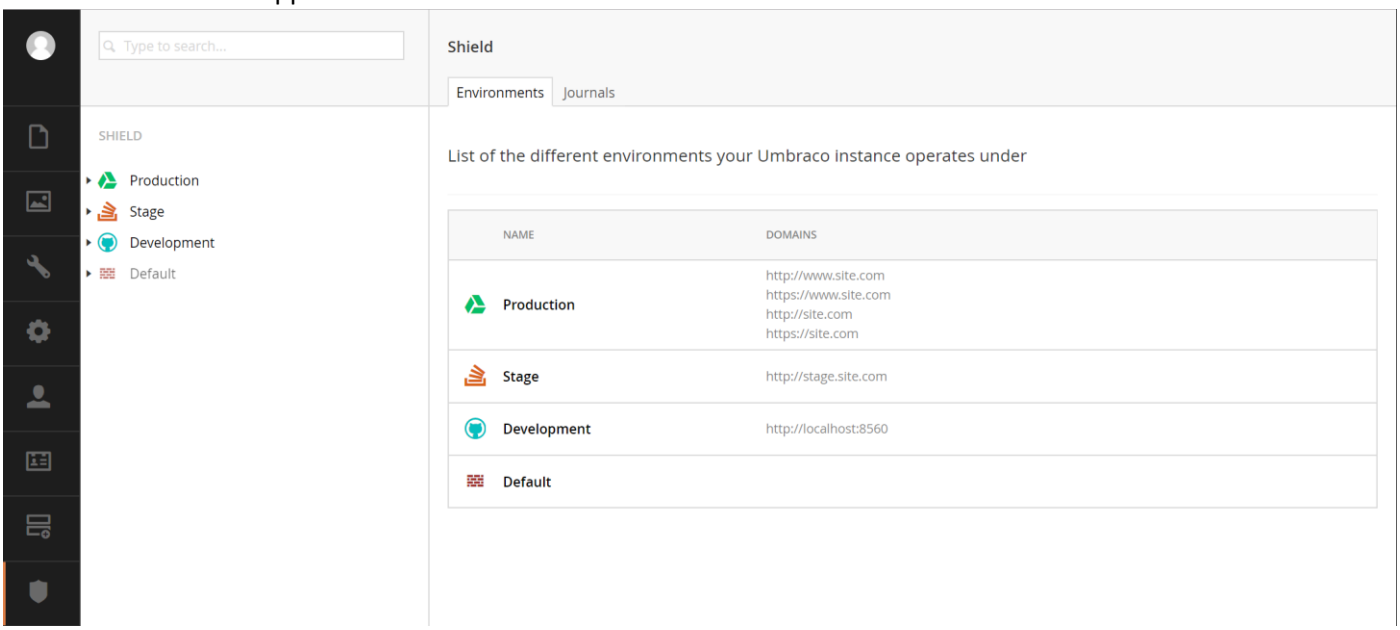


Afterwards, Shield should be installed

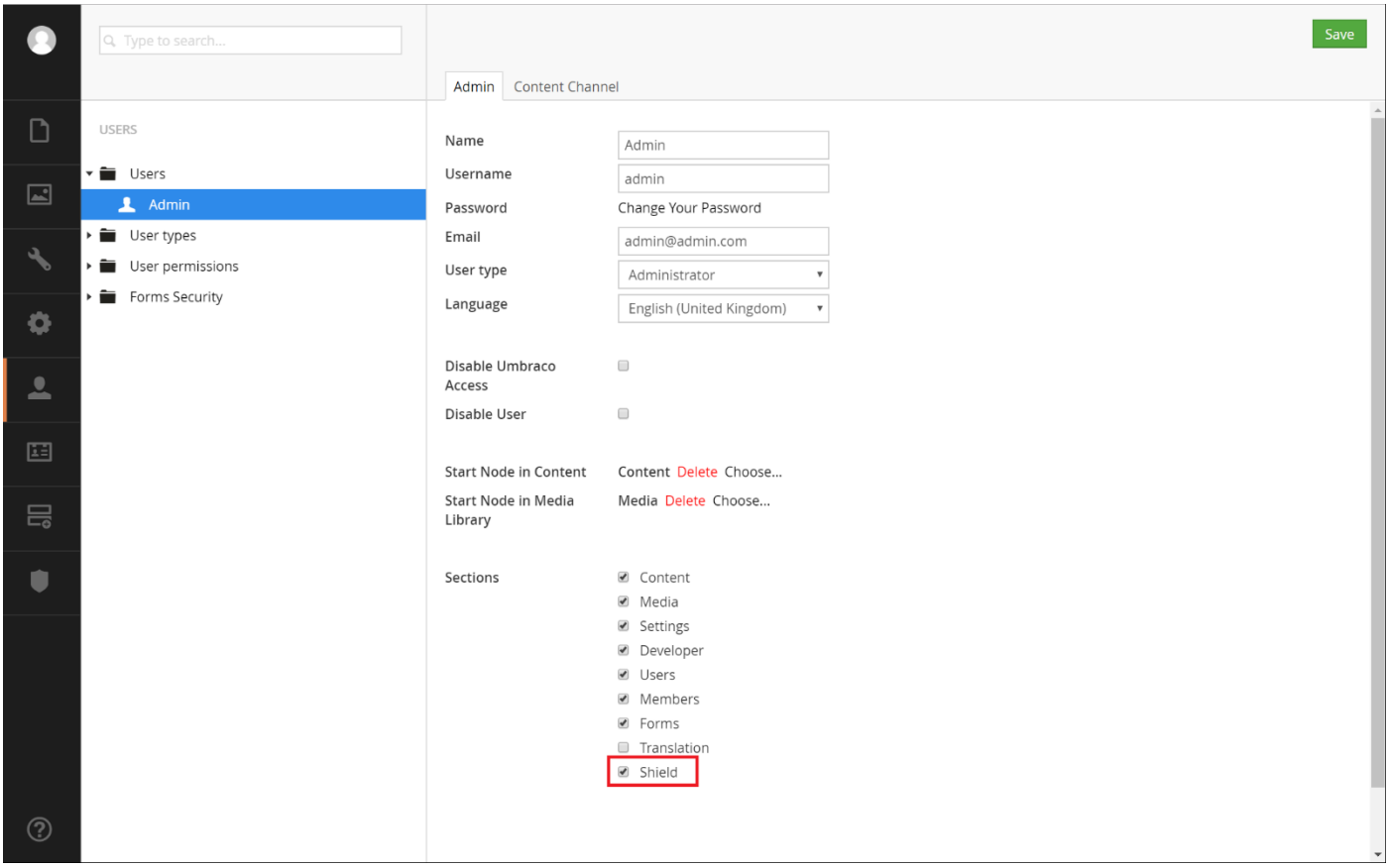
Shield

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'll be given a new custom section within the backoffice of Umbraco to modify shields behaviour as needed based on the apps installed.



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

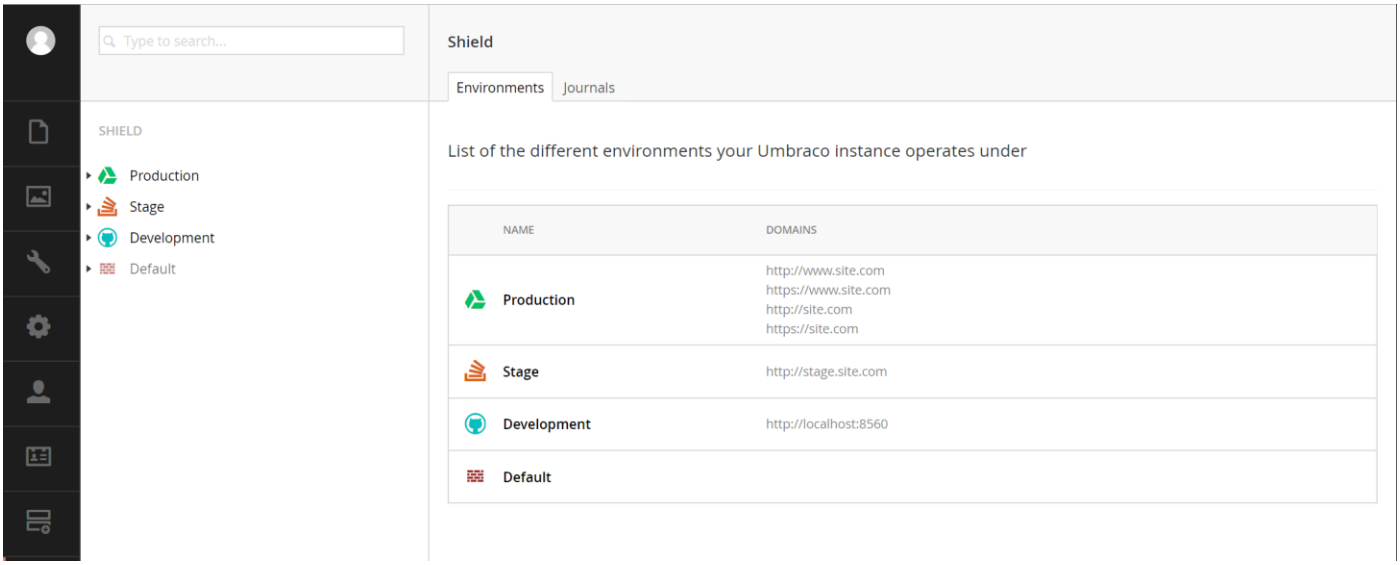


In newer version of Umbraco v7, you'll need to add Shield section via the User Group which the current logged in user is applied to.

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.

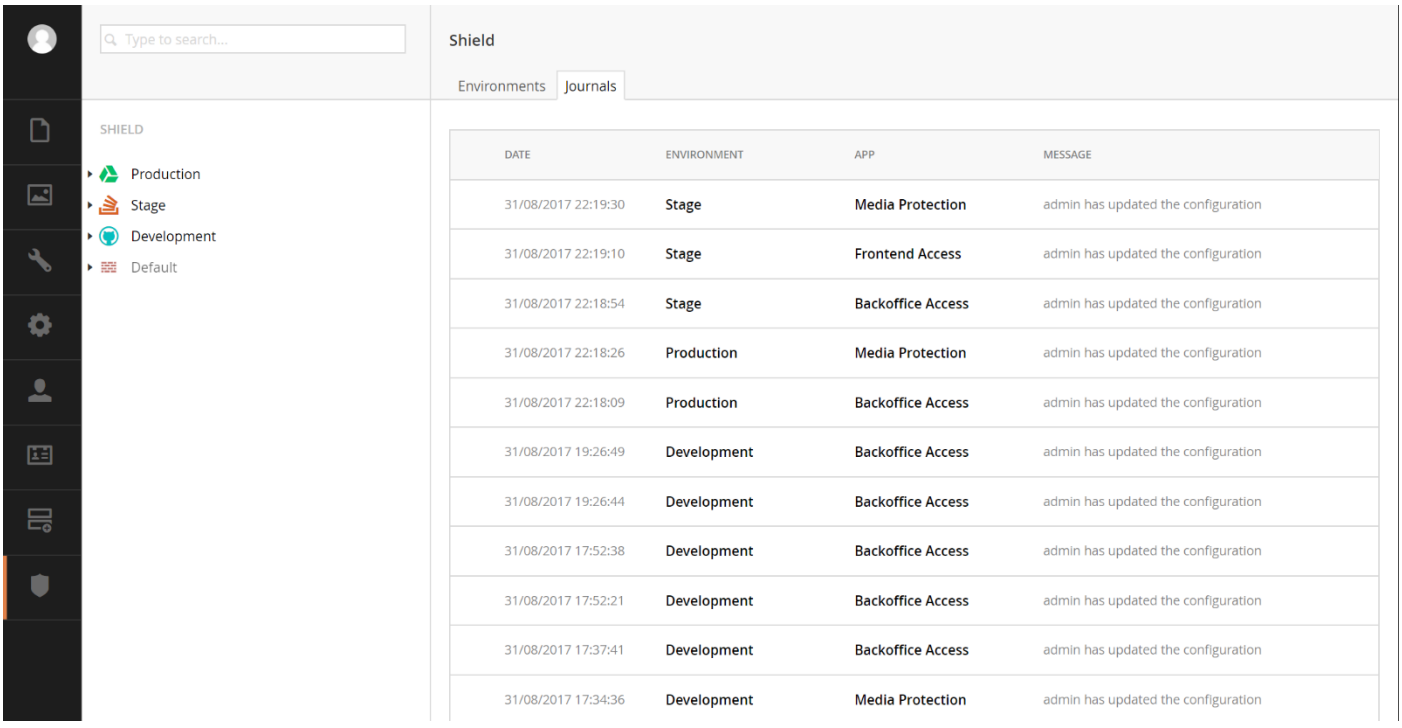
This allows different configuration of apps for your different environments; for example, Hot Linking protection only on your Production environment and Frontend Access restrictions on your Staging environment.



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:

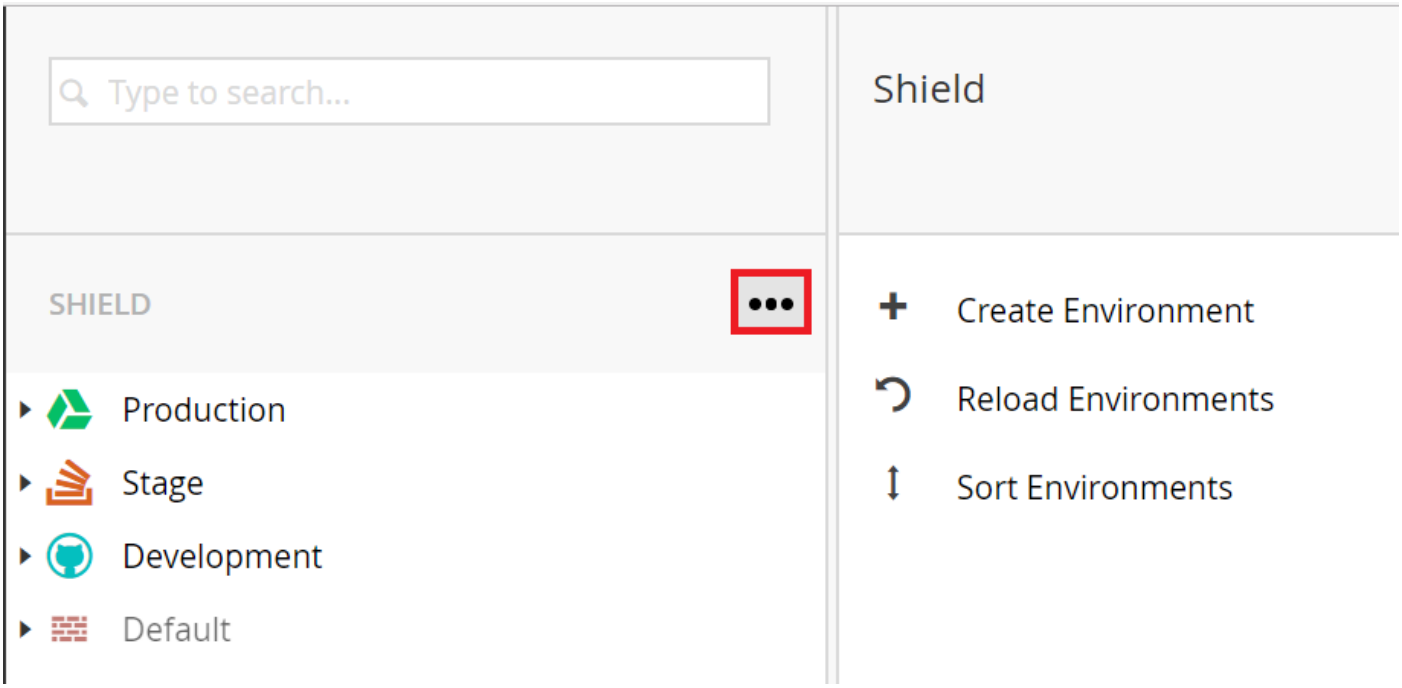
- Date & time (UTC) of when the Journal item was created
- The environment of the app that created the Journal item
- The app that created the Journal item
- A message of why the Journal item was created



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

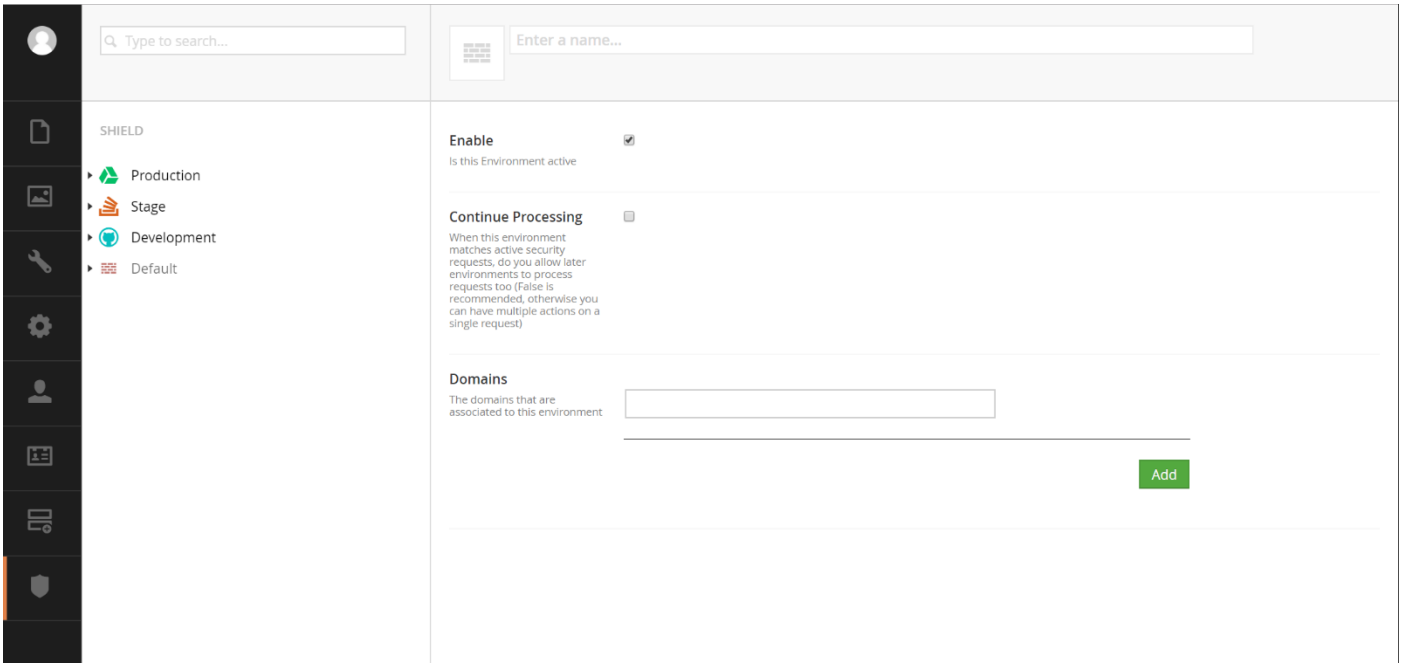
Create Environment

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

- Select an **Icon** that identifies visually this environment
- Set a 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 and 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

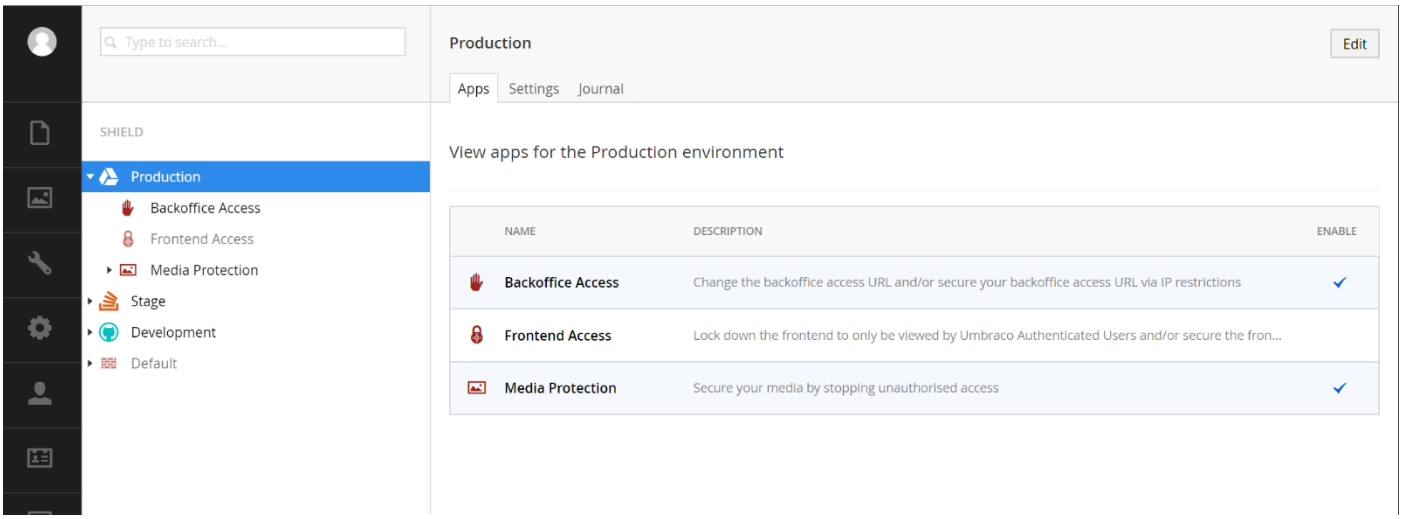
The reason for Production being first, is that this will, ever so slightly, be processed first and will speed up any Live requests – which normally is more important, but it is all very marginal.

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.

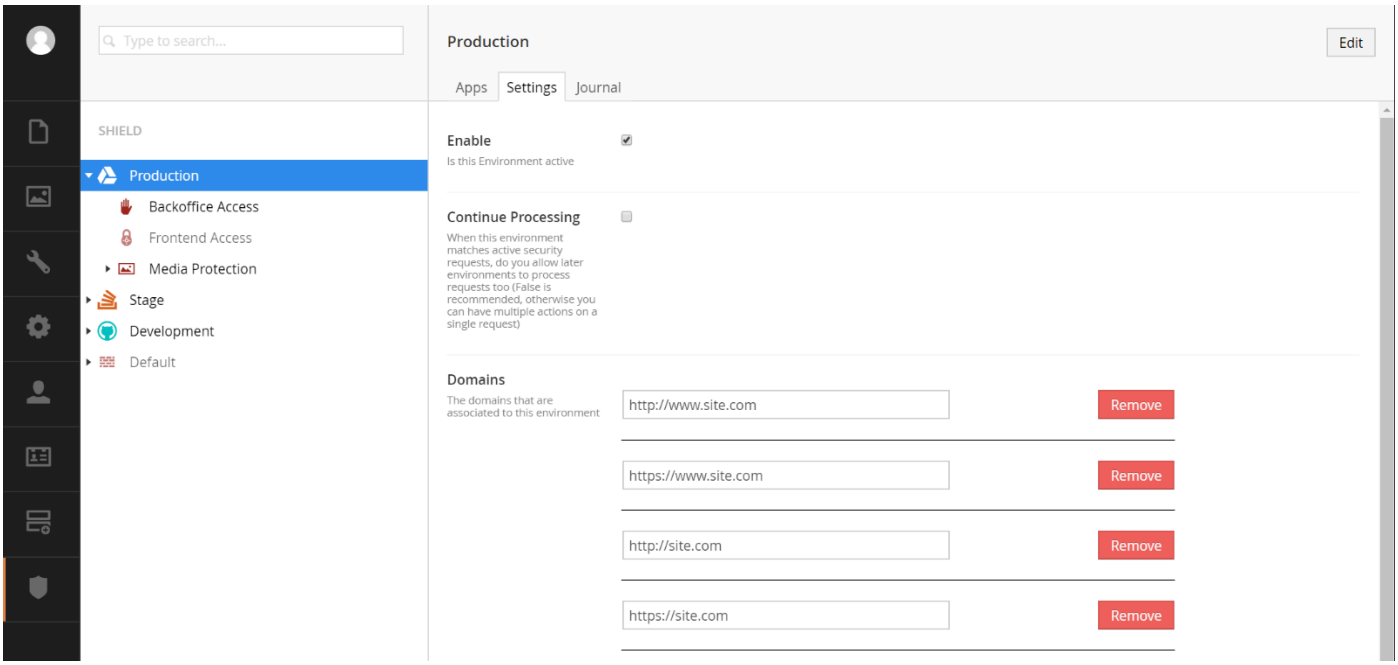
Apps

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.



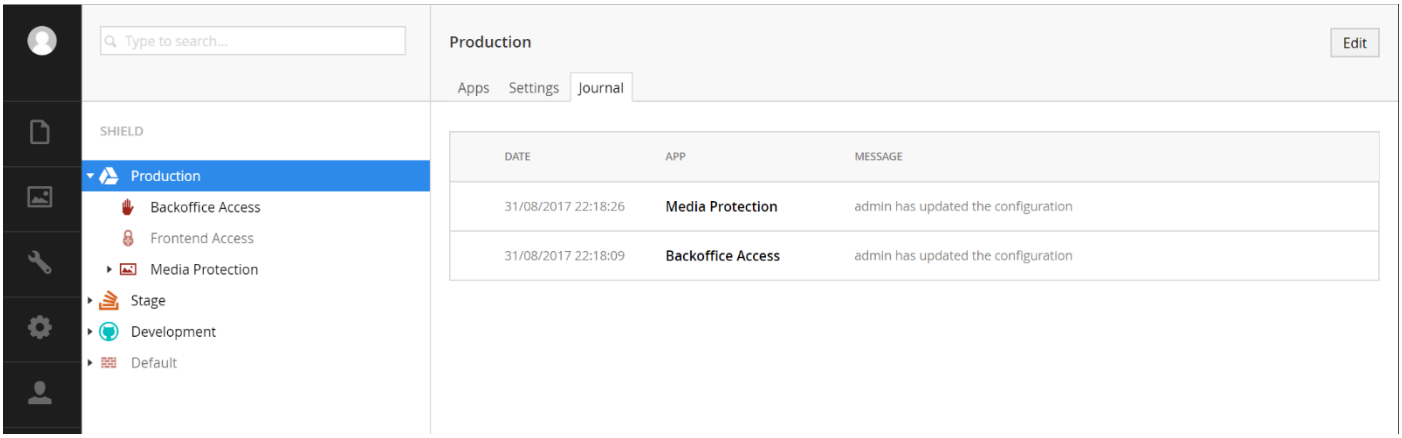
Settings

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.



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.

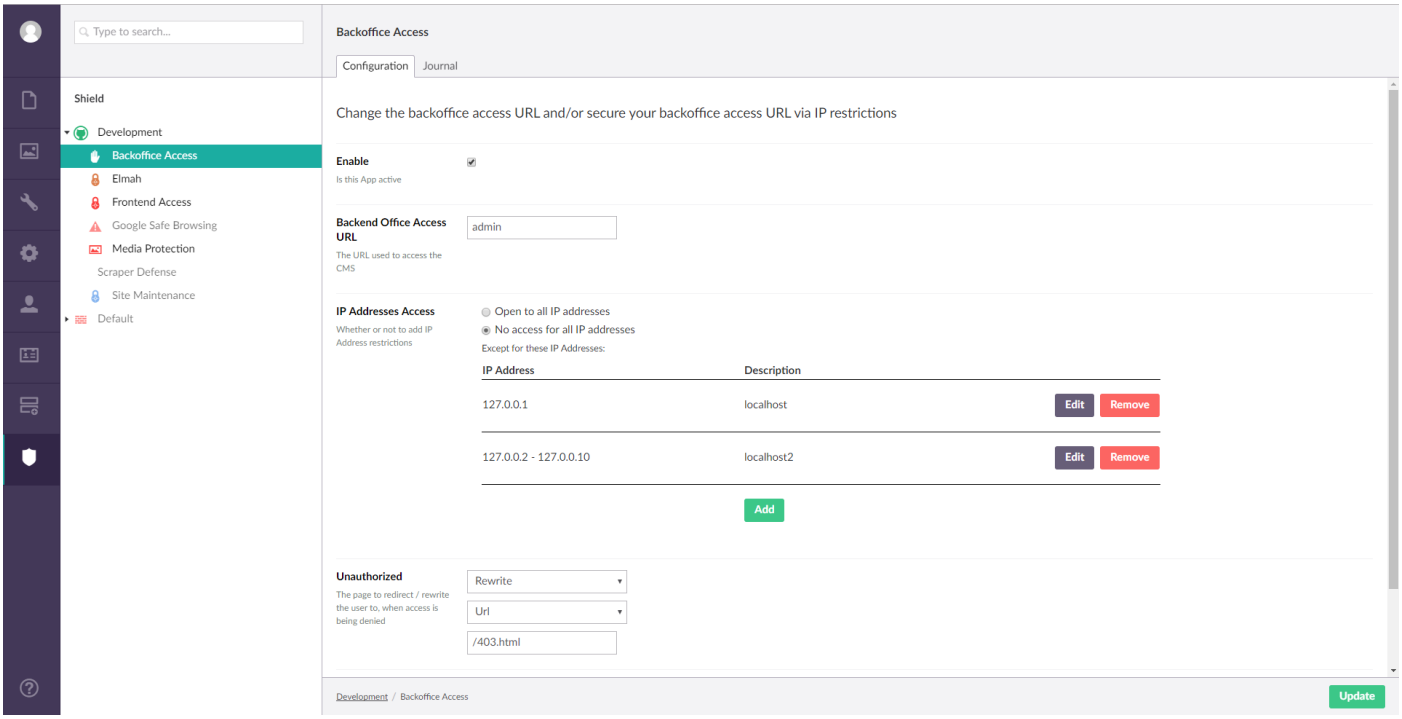


Backoffice Access

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/black-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 and cannot be a subdomain.
- Whether the backoffice is accessible by all IP Addresses or to specific IP Addresses with the ability to define a whitelist or blacklist of IP Address(es).
- Whether to play dead, redirect or rewrite the request to another location.
- The URL to redirect or rewrite the request to.



Journal

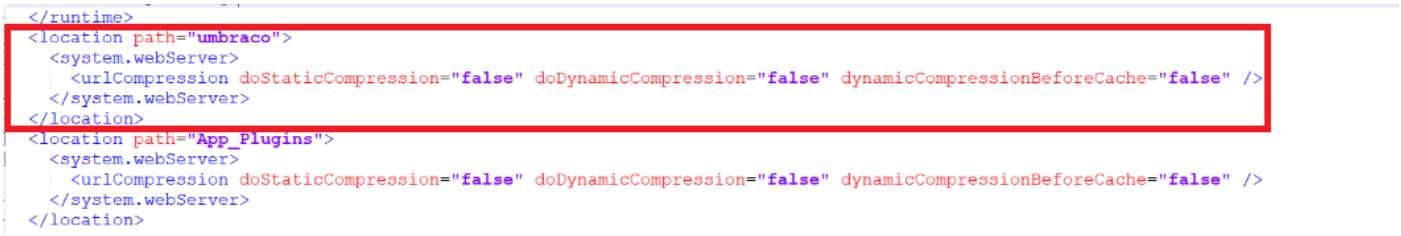
Like the Journal Dashboard, this will only show the journal entries for the selected app & environment. The list will show warnings, messages and errors that have occurred within the app. This includes all unauthorised attempts to gain access to the backoffice access URL.

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="umbracoHideTopLevelNodeFromPath" value="true" />
  <add key="umbracoUseDirectoryUrls" value="true" />
  <add key="umbracoTimeOutInMinutes" value="60" />
```

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



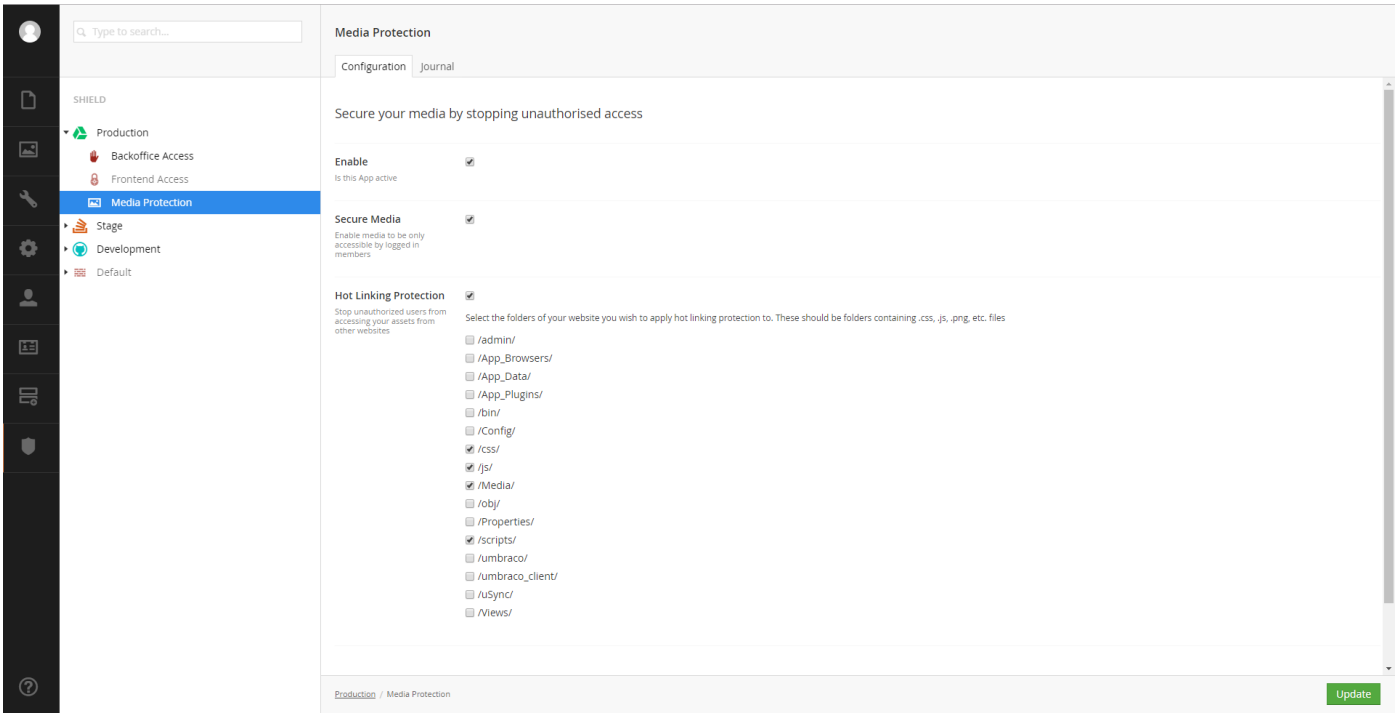
This is because, as part of Backoffice Access functionality, it will set these to whatever your preferred access URL is. You should then be able to upgrade Umbraco the normal way via the installer/upgrader, using the URL '/umbraco'. Once the upgrade process has been completed, you'll find '/umbraco' 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.



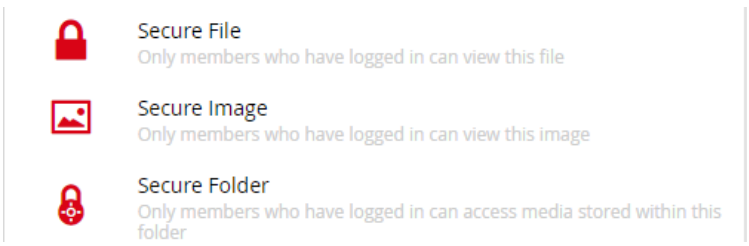
Journal

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.

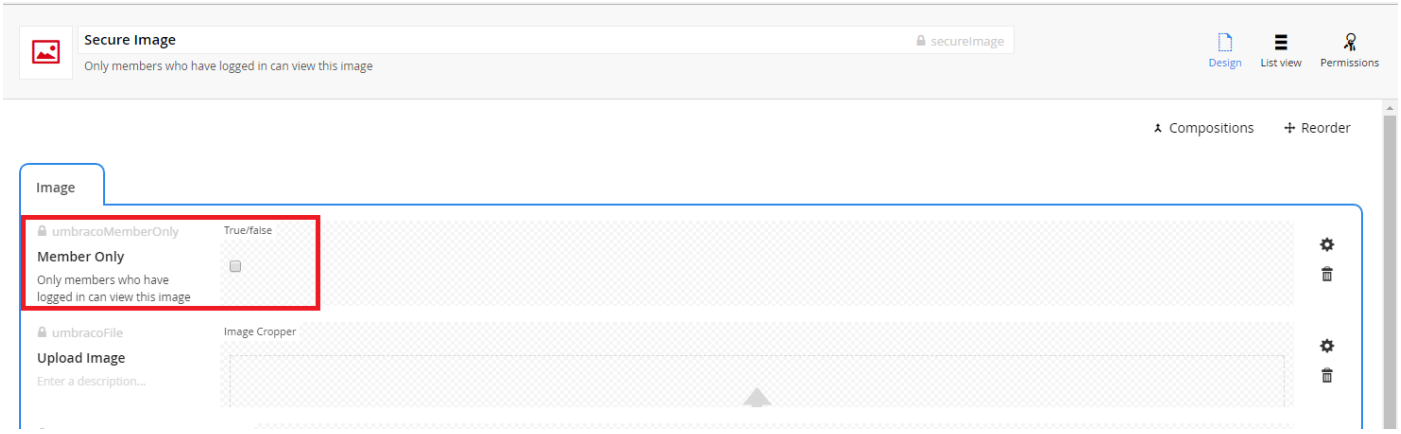
Media Types

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" (or in newer versions of Umbraco v7, the checkbox data-type).



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

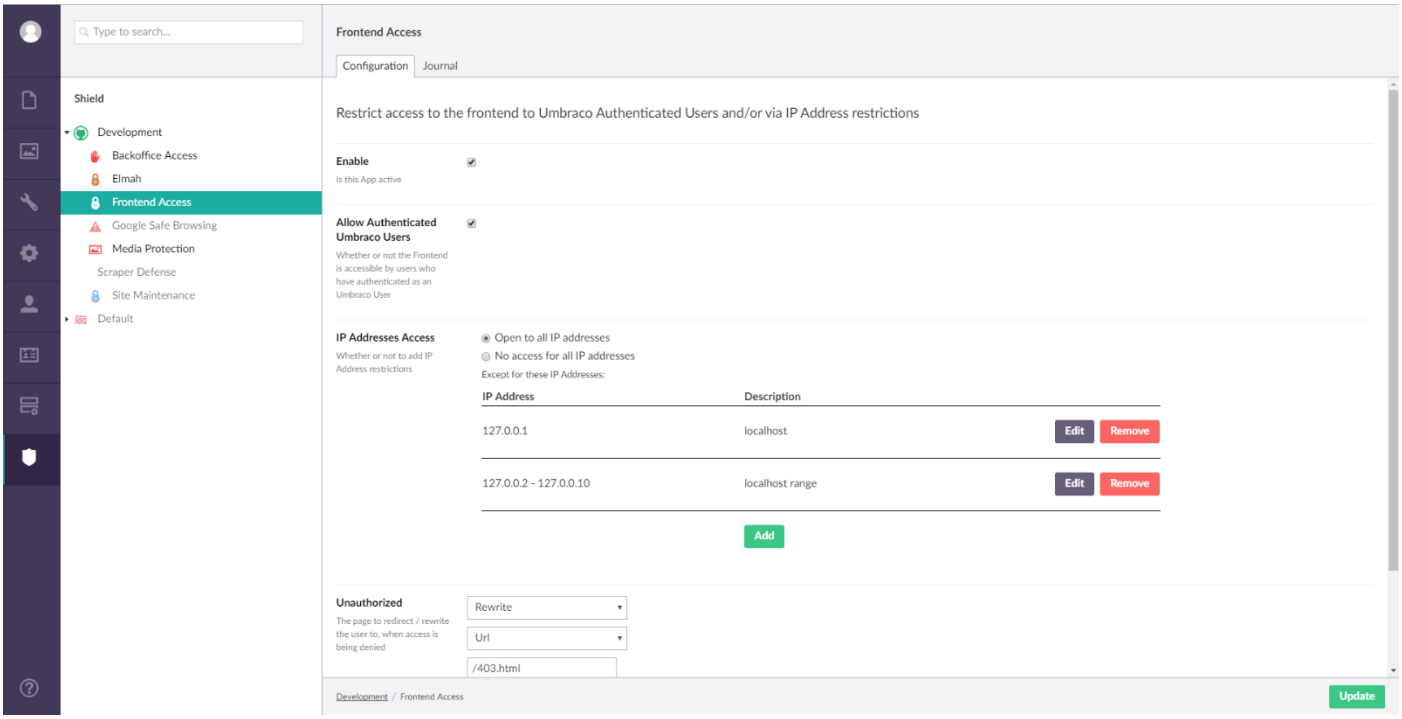
And on the Secure Folder, you have the "Member Only" tickbox checked, then all the children, (the x1 Secure Image & the x2 Image) will only be accessible by authenticated users. The x1 Secure Image item itself doesn't need the "Member Only" tickbox checked.

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 with the ability to define a whitelist or blacklist of IP Address(es).
- Whether to play dead, redirect or rewrite the request to another location.
- The URL to redirect or rewrite the request to.



Journal

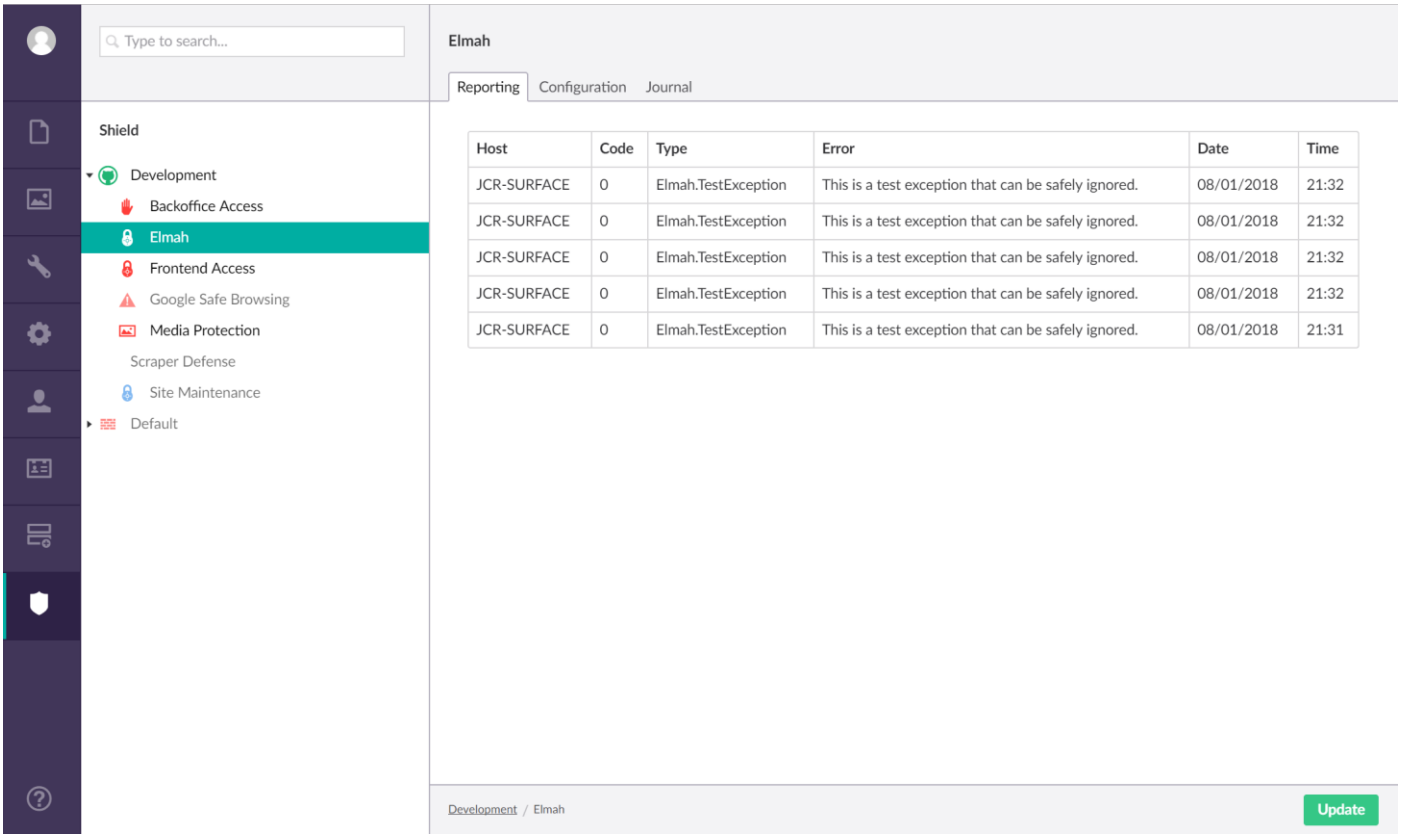
Similar to the Journal Dashboard, this will only show the journal entries for the selected app & environment. The list will show warnings, messages and errors that have occurred within the app. This includes all unauthorised attempts to gain access to the front end of the website.

Elmah

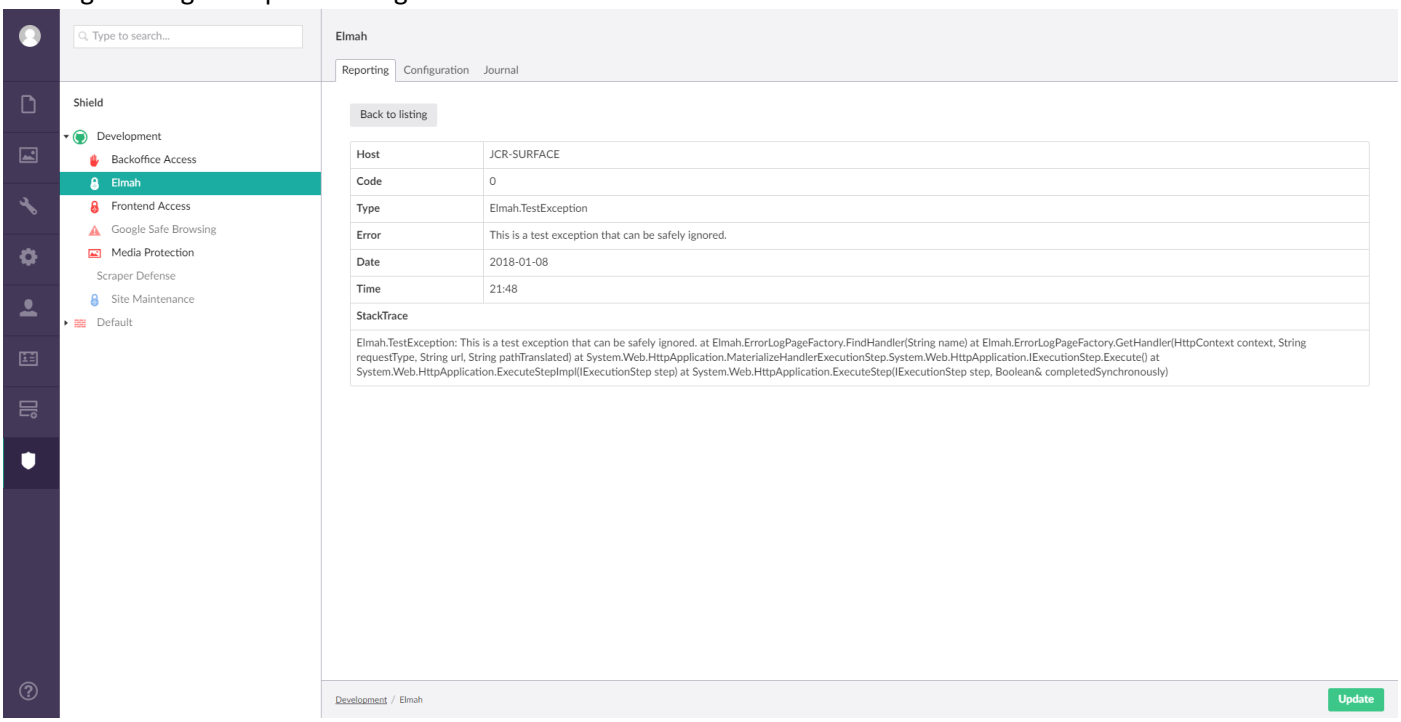
Elmah adds the popular error logging library ELMAH to Umbraco and allows you to restrict access to ~/elmah.axd

Reporting

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

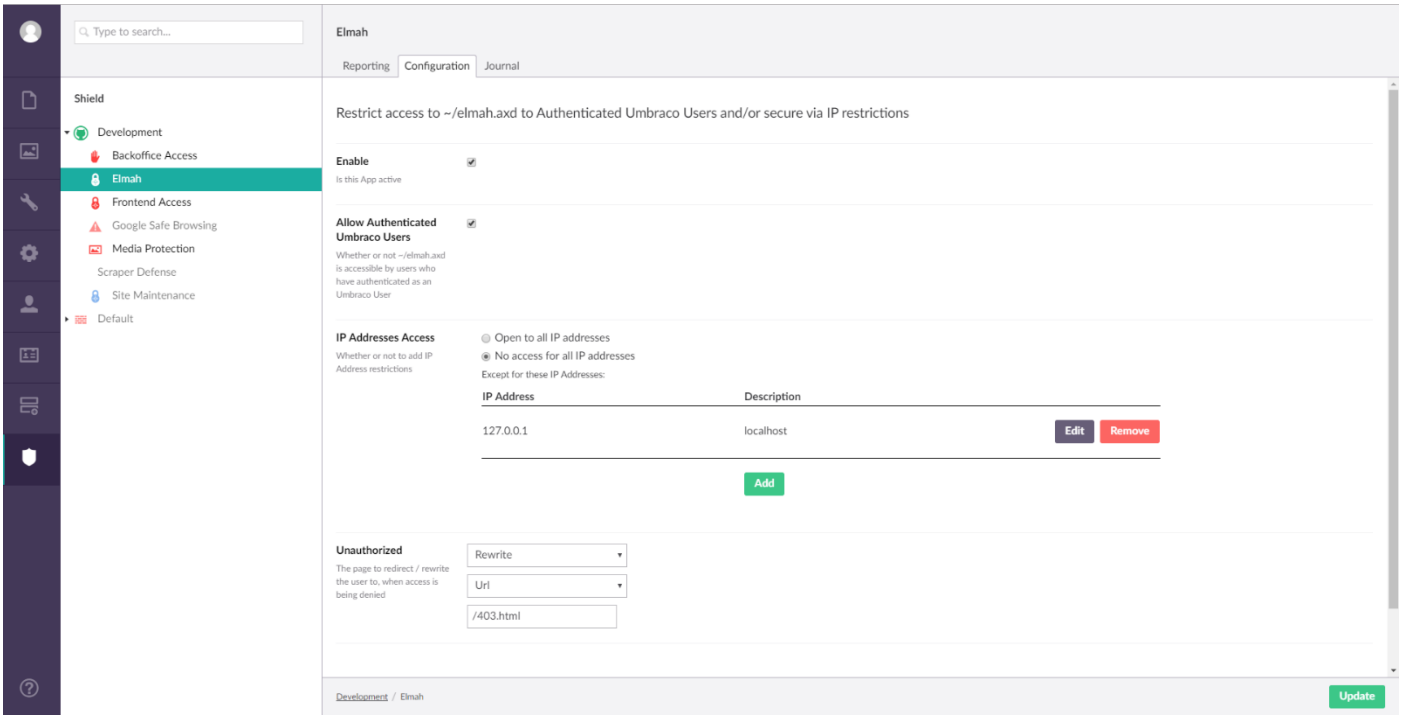


Clicking on a log will open that log and show more details about the error.



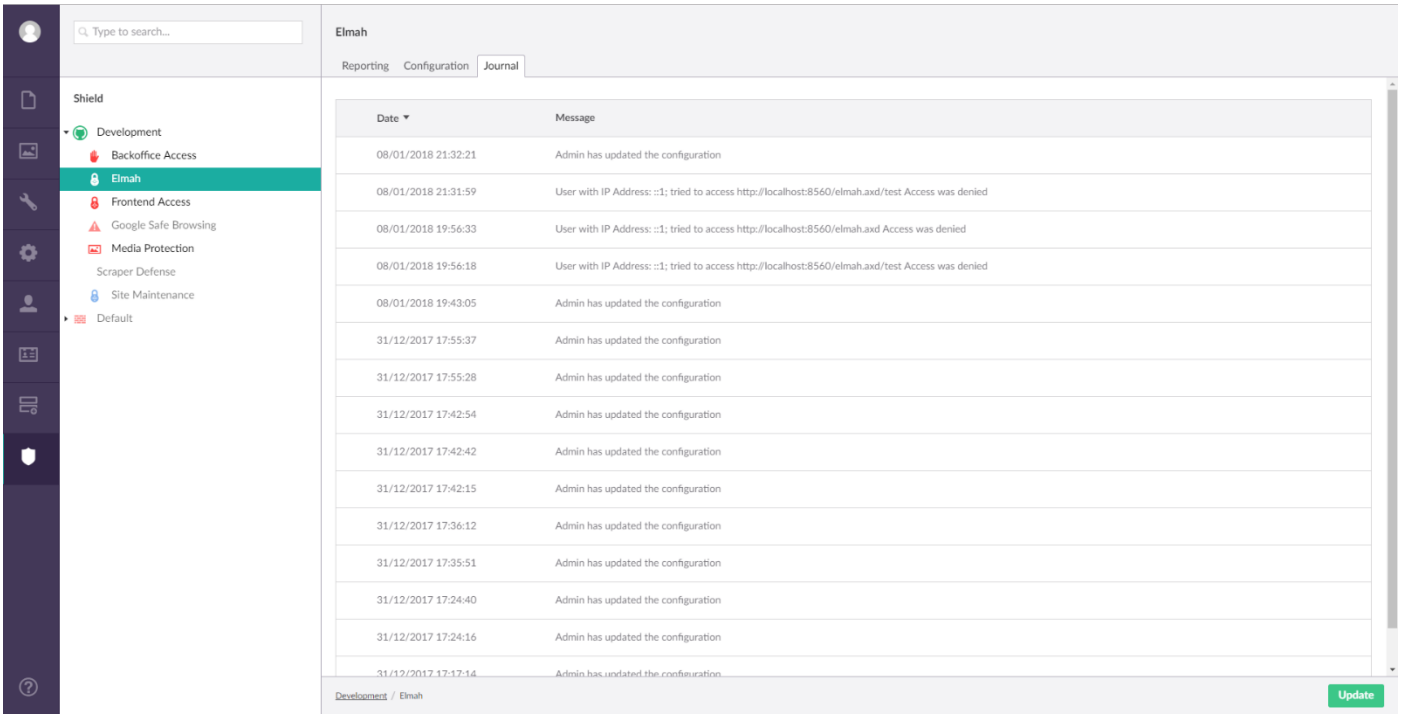
Configuration

- 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 with the ability to define a whitelist or blacklist of IP Address(es).
- Whether to play dead, redirect or rewrite the request to another location.
- The URL to redirect or rewrite the request to.



Journal

Like 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 ~/elmah.axd URL.

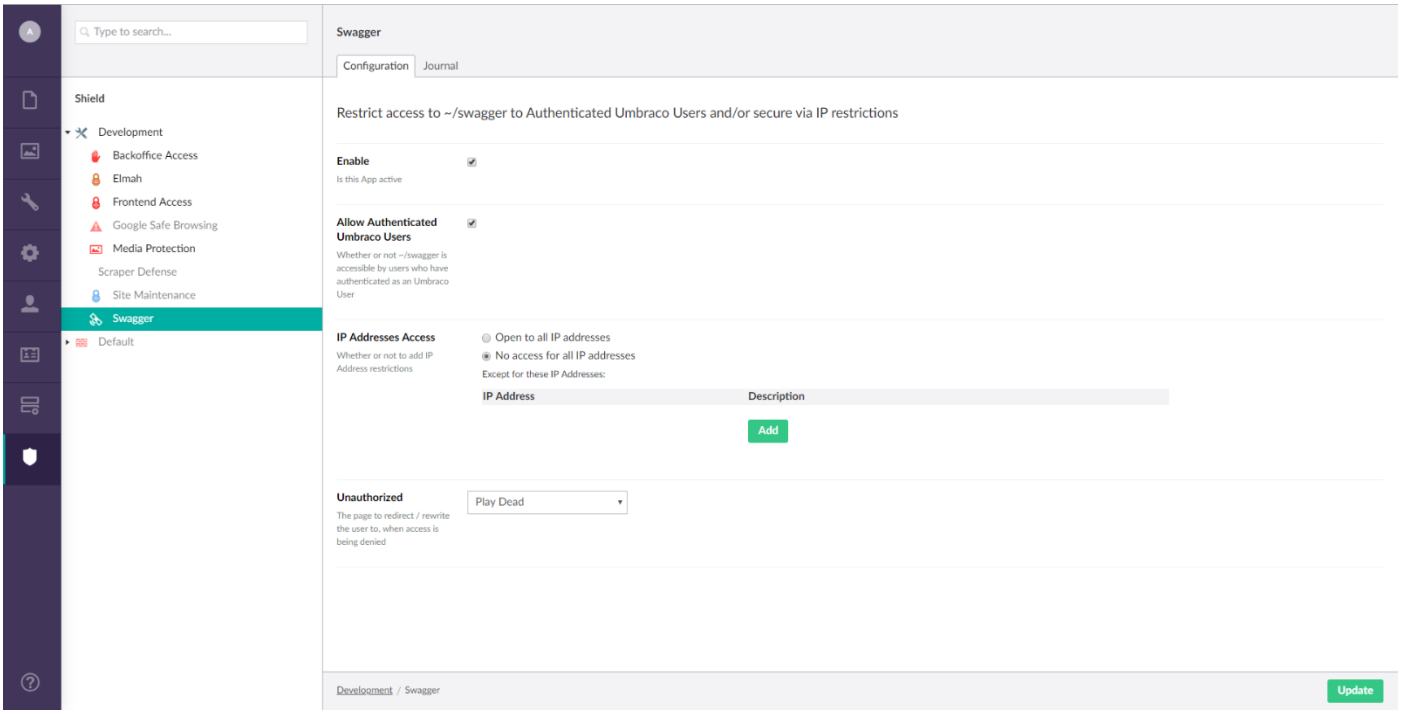


Swagger

Swagger adds https://swagger.io/ to your Umbraco installation, configured to ignore Umbraco's API's and allows you to restrict access to authenticated Umbraco users and/or a whitelist or blacklist of IP addresses.

Configuration

- The ability to enable/disable this app. When disable, ~/swagger will be inaccessible even though being installed. When enabled, ~/swagger can be accessed depending on the app's configuration.
- Whether ~/swagger is accessible by authenticated Umbraco users.
- Whether ~/swagger is accessible by all IP Addresses or to specific IP Addresses with the ability to define a whitelist or blacklist of IP Address(es)
- Whether to play dead, redirect or rewrite the request to another location.
- The URL to redirect or rewrite the request to.



Journal

Like 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 ~/swagger URL.

Installation

Umbraco Package Manager

If installed via the Umbraco Package Manager, you don't need to do anything further.

Nuget

Once installed, you'll need to either do one of the following regardless of having Swashbuckle installed prior or as part of installing Our.Shield.Swagger:

- Remove the SwaggerConfig.cs file that comes with Swashbuckle nuget package (this should be installed to the App_Start folder of the project)
  OR
- Within your Application Starting event handler call methods:
  - `GlobalConfiguration.Configuration.SetSwaggerDocsConfig()`
    AND/OR
  - `GlobalConfiguration.Configuration.SetSwaggerUiConfig()`

  Providing the corresponding configuration you'd like