

---

# **Ocelot**

## ***Release 21.0***

**Tom Pallister, Ocelot Core team at ThreeMammals**

**Feb 16, 2024**



# INTRODUCTION

<b>1</b>	<b>Big Picture</b>	<b>3</b>
1.1	Basic Implementation . . . . .	4
1.2	With IdentityServer . . . . .	4
1.3	Multiple Instances . . . . .	5
1.4	With Consul . . . . .	5
1.5	With Service Fabric . . . . .	6
<b>2</b>	<b>Getting Started</b>	<b>7</b>
2.1	.NET 8.0 . . . . .	7
<b>3</b>	<b>Contributing</b>	<b>11</b>
<b>4</b>	<b>Not Supported</b>	<b>13</b>
4.1	Chunked Encoding . . . . .	13
4.2	Forwarding a Host header . . . . .	13
4.3	Swagger . . . . .	13
<b>5</b>	<b>Gotchas</b>	<b>15</b>
5.1	IIS . . . . .	15
<b>6</b>	<b>Administration</b>	<b>17</b>
6.1	Providing your own IdentityServer . . . . .	17
6.2	Internal IdentityServer . . . . .	18
6.3	Administration API . . . . .	19
<b>7</b>	<b>Authentication</b>	<b>21</b>
7.1	JWT Tokens . . . . .	21
7.2	Identity Server Bearer Tokens . . . . .	22
7.3	Auth0 by Okta . . . . .	23
7.4	Allowed Scopes . . . . .	23
7.5	More identity providers . . . . .	23
<b>8</b>	<b>Authorization</b>	<b>25</b>
8.1	Authorization Middleware . . . . .	25
<b>9</b>	<b>Caching</b>	<b>27</b>
9.1	Your Own Caching . . . . .	28
<b>10</b>	<b>Claims Transformation</b>	<b>29</b>
10.1	Claims to Claims Transformation . . . . .	29
10.2	Claims to Headers Tranformation . . . . .	30

10.3	Claims to Query String Parameters Transformation . . . . .	30
10.4	Claims to Downstream Path Transformation . . . . .	30
<b>11</b>	<b>Configuration</b>	<b>31</b>
11.1	Multiple Environments . . . . .	32
11.2	Merging Configuration Files . . . . .	33
11.3	Store Configuration in Consul . . . . .	34
11.4	Reload JSON Config On Change . . . . .	34
11.5	Configuration Key . . . . .	34
11.6	Follow Redirects aka HttpHandlerOptions . . . . .	35
11.7	SSL Errors . . . . .	35
11.8	React to Configuration Changes . . . . .	36
11.9	DownstreamHttpVersion . . . . .	37
<b>12</b>	<b>Delegating Handlers</b>	<b>39</b>
12.1	How to Use . . . . .	39
12.2	Order of Execution . . . . .	40
<b>13</b>	<b>Dependency Injection</b>	<b>41</b>
13.1	Overview . . . . .	41
13.2	IServiceCollection extensions . . . . .	41
13.3	The OcelotBuilder class . . . . .	42
13.4	Custom Builder . . . . .	44
<b>14</b>	<b>Error Status Codes</b>	<b>47</b>
14.1	Client error responses . . . . .	47
14.2	Server error responses . . . . .	47
14.3	Design . . . . .	47
<b>15</b>	<b>GraphQL</b>	<b>49</b>
15.1	Future . . . . .	49
<b>16</b>	<b>Headers Transformation</b>	<b>51</b>
16.1	Add to Request . . . . .	51
16.2	Add to Response . . . . .	51
16.3	Find and Replace . . . . .	52
16.4	Pre Downstream Request . . . . .	52
16.5	Post Downstream Request . . . . .	52
16.6	Placeholders . . . . .	52
16.7	Handling 302 Redirects . . . . .	53
16.8	X-Forwarded-For . . . . .	53
16.9	Future . . . . .	53
<b>17</b>	<b>Kubernetes</b>	<b>55</b>
<b>18</b>	<b>Load Balancer</b>	<b>57</b>
18.1	Configuration . . . . .	57
18.2	Service Discovery . . . . .	58
18.3	CookieStickySessions Type . . . . .	58
18.4	Custom Load Balancers . . . . .	59
<b>19</b>	<b>Logging</b>	<b>61</b>
19.1	Warning . . . . .	61
<b>20</b>	<b>Method Transformation</b>	<b>63</b>

<b>21</b>	<b>Middleware Injection</b>	<b>65</b>
21.1	ASP.NET Core Middlewares and Ocelot Pipeline Builder . . . . .	66
21.2	Future . . . . .	66
<b>22</b>	<b>Quality of Service</b>	<b>67</b>
<b>23</b>	<b>Rate Limiting</b>	<b>69</b>
23.1	Ocelot Own Implementation . . . . .	69
23.2	Future and ASP.NET Core Implementation . . . . .	70
<b>24</b>	<b>Request Aggregation</b>	<b>71</b>
24.1	Advanced Register Your Own Aggregators . . . . .	71
24.2	Basic Expecting JSON from Downstream Services . . . . .	73
24.3	Gotchas . . . . .	74
<b>25</b>	<b>Request ID</b>	<b>75</b>
25.1	Global . . . . .	75
25.2	Route . . . . .	75
25.3	Gotcha . . . . .	75
<b>26</b>	<b>Routing</b>	<b>77</b>
26.1	Placeholders . . . . .	78
26.2	Catch All . . . . .	78
26.3	Upstream Host . . . . .	79
26.4	Priority . . . . .	79
26.5	Dynamic Routing . . . . .	80
26.6	Query Strings . . . . .	80
26.7	Security Options . . . . .	81
<b>27</b>	<b>Service Discovery</b>	<b>83</b>
27.1	Consul . . . . .	83
27.2	Eureka . . . . .	85
27.3	Dynamic Routing . . . . .	86
27.4	Custom Providers . . . . .	88
<b>28</b>	<b>Service Fabric</b>	<b>91</b>
<b>29</b>	<b>Tracing</b>	<b>93</b>
29.1	OpenTracing . . . . .	93
29.2	Butterfly . . . . .	94
<b>30</b>	<b>Websockets</b>	<b>95</b>
30.1	Links . . . . .	95
30.2	SignalR . . . . .	96
30.3	Supported . . . . .	96
30.4	Not Supported . . . . .	97
30.5	Future . . . . .	97
<b>31</b>	<b>Overview</b>	<b>99</b>
<b>32</b>	<b>Building</b>	<b>101</b>
<b>33</b>	<b>Tests</b>	<b>103</b>
33.1	Create SSL Cert for Testing . . . . .	103

**34 Release Process** **105**

34.1 Notes . . . . . 106

34.2 Quality Gates . . . . . 106

Thanks for taking a look at the Ocelot documentation! Please use the left hand navigation to get around. The team would suggest taking a look at the **Introduction** chapter first.

All **Features** are arranged in alphabetical order. The main features are *Configuration* and *Routing*.

We **do** follow development process which is described in *Release Process*.





## **BIG PICTURE**

Ocelot is aimed at people using .NET running a microservices / service-oriented architecture that need a unified point of entry into their system. However it will work with anything that speaks HTTP(S) and run on any platform that ASP.NET Core supports.

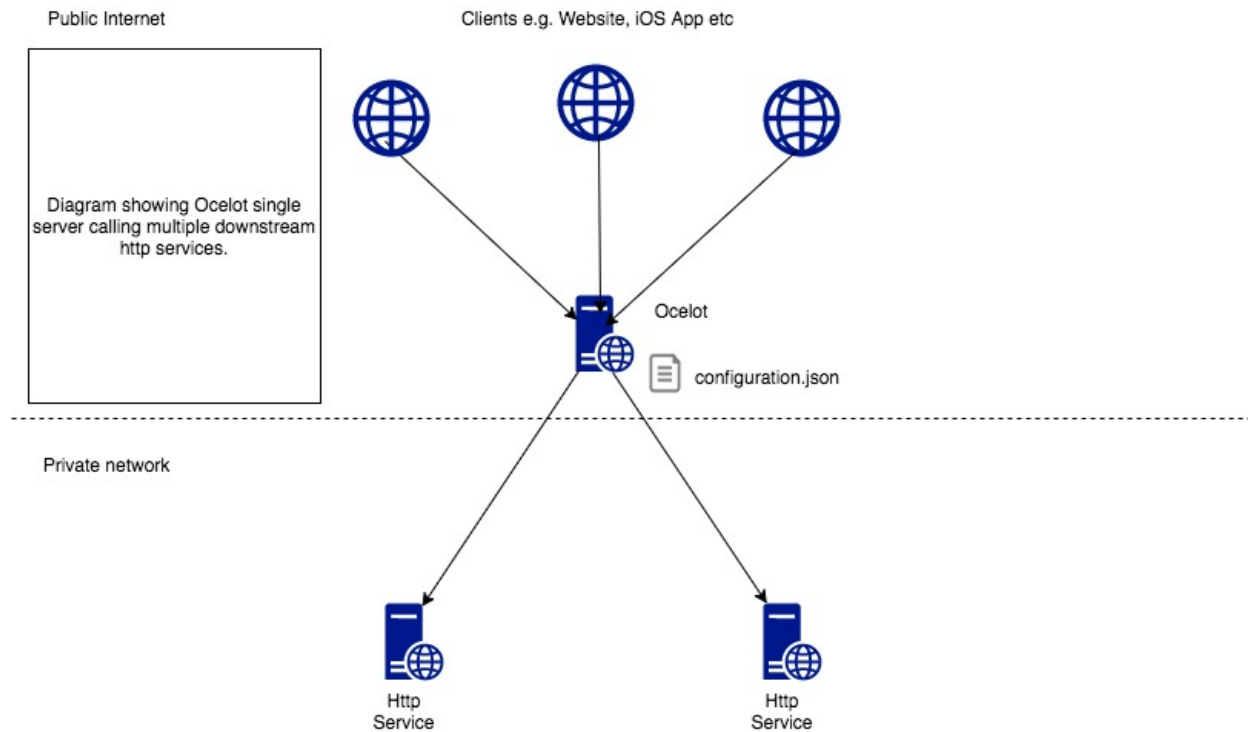
In particular we want easy integration with [IdentityServer](#) reference and [Bearer](#) tokens. We have been unable to find this in our current workplace without having to write our own Javascript middlewares to handle the IdentityServer reference tokens. We would rather use the IdentityServer code that already exists to do this.

Ocelot is a bunch of middlewares in a specific order.

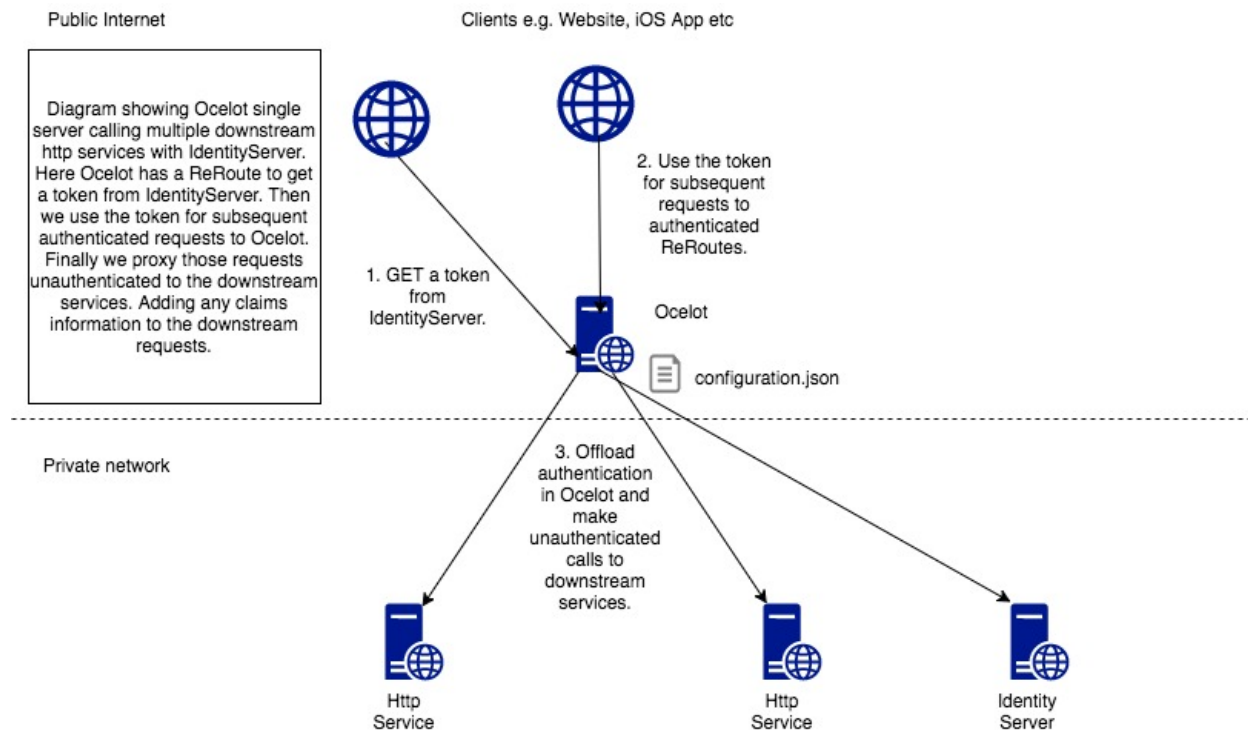
Ocelot manipulates the `HttpRequest` object into a state specified by its configuration until it reaches a request builder middleware, where it creates a `HttpRequestMessage` object which is used to make a request to a downstream service. The middleware that makes the request is the last thing in the Ocelot pipeline. It does not call the next middleware. The response from the downstream service is retrieved as the requests goes back up the Ocelot pipeline. There is a piece of middleware that maps the `HttpResponseMessage` onto the `HttpResponse` object and that is returned to the client. That is basically it with a bunch of other features!

The following are configurations that you use when deploying Ocelot.

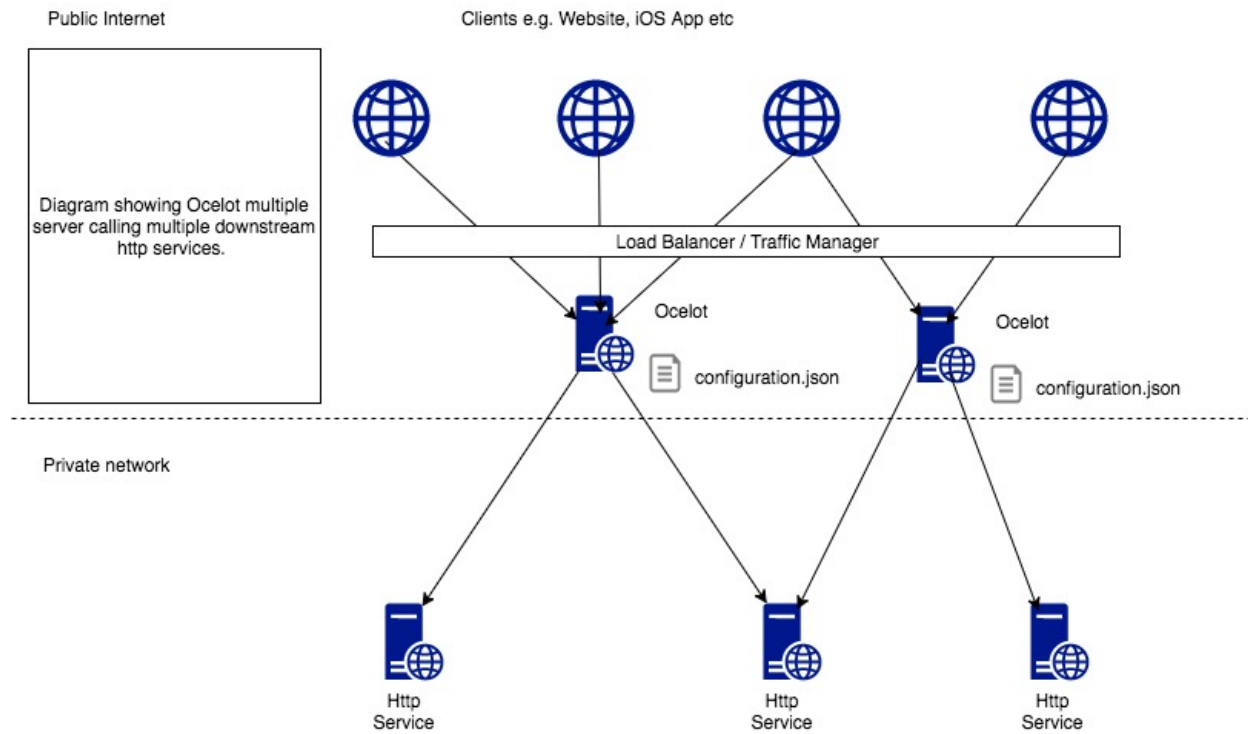
## 1.1 Basic Implementation



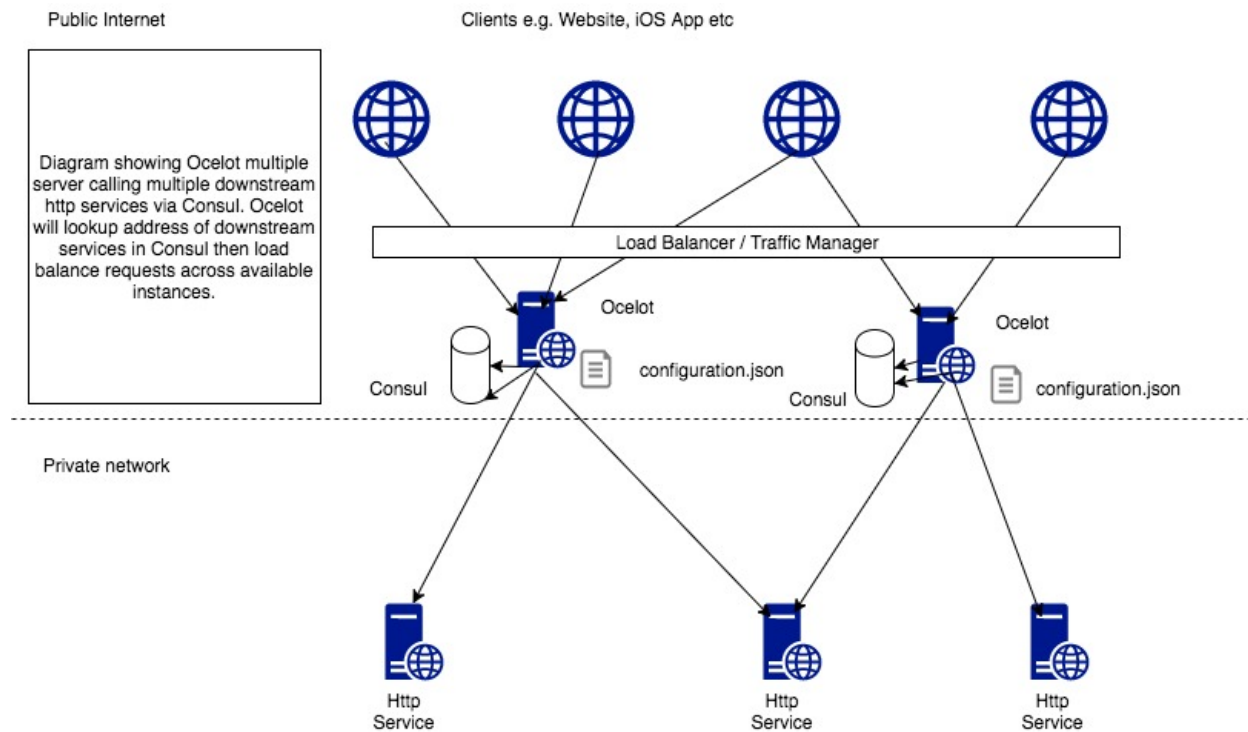
## 1.2 With IdentityServer



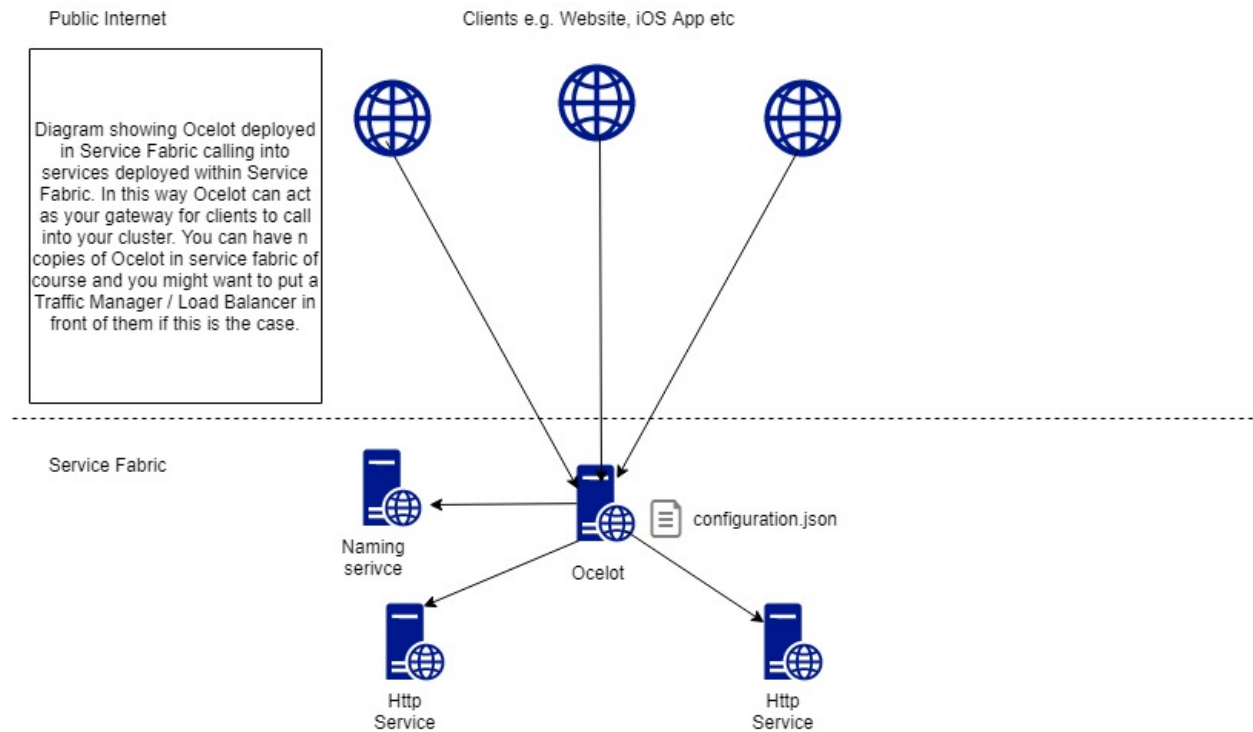
## 1.3 Multiple Instances



## 1.4 With Consul



## 1.5 With Service Fabric



## GETTING STARTED

Ocelot is designed to work with ASP.NET and is currently on `net6.0`, `net7.0` and `net8.0` frameworks.

### 2.1 .NET 8.0

#### 2.1.1 Install NuGet package

Install Ocelot and its dependencies using [NuGet](#). You will need to create a [ASP.NET Core minimal API project](#) and bring the package into it. Then follow the startup below and [Configuration](#) sections to get up and running.

`Install-Package` Ocelot

All versions can be found in the [NuGet Gallery | Ocelot](#).

#### 2.1.2 Configuration

The following is a very basic **ocelot.json**. It won't do anything but should get Ocelot starting.

```
{
  "Routes": [],
  "GlobalConfiguration": {
    "BaseUrl": "https://api.mybusiness.com"
  }
}
```

If you want some example that actually does something use the following:

```
{
  "Routes": [
    {
      "DownstreamPathTemplate": "/todos/{id}",
      "DownstreamScheme": "https",
      "DownstreamHostAndPorts": [
        {
          "Host": "jsonplaceholder.typicode.com",
          "Port": 443
        }
      ],
      "UpstreamPathTemplate": "/todos/{id}",

```

(continues on next page)

(continued from previous page)

```

        "UpstreamHttpMethod": [ "Get" ]
    },
    "GlobalConfiguration": {
        "BaseUrl": "https://localhost:5000"
    }
}

```

The most important thing to note here is **BaseUrl** property. Ocelot needs to know the URL it is running under in order to do Header find & replace and for certain administration configurations. When setting this URL it should be the external URL that clients will see Ocelot running on e.g. If you are running containers Ocelot might run on the URL `http://123.12.1.1:6543` but has something like **nginx** in front of it responding on `https://api.mybusiness.com`. In this case the Ocelot **BaseUrl** should be `https://api.mybusiness.com`.

If you are using containers and require Ocelot to respond to clients on `http://123.12.1.1:6543` then you can do this, however if you are deploying multiple Ocelot's you will probably want to pass this on the command line in some kind of script. Hopefully whatever scheduler you are using can pass the IP.

## 2.1.3 Program

Then in your **Program.cs** you will want to have the following. The main things to note are `AddOcelot()`<sup>1</sup> (adds Ocelot default services), `UseOcelot().Wait()` (sets up all the Ocelot middleware).

```

using System.IO;
using Microsoft.AspNetCore.Hosting;
using Microsoft.Extensions.Configuration;
using Microsoft.Extensions.Hosting;
using Ocelot.DependencyInjection;
using Ocelot.Middleware;

namespace OcelotBasic
{
    public class Program
    {
        public static void Main(string[] args)
        {
            new WebHostBuilder()
                .UseKestrel()
                .UseContentRoot(Directory.GetCurrentDirectory())
                .ConfigureAppConfiguration((hostingContext, config) =>
                {
                    config
                        .SetBasePath(hostingContext.HostingEnvironment.ContentRootPath)
                        .AddJsonFile("appsettings.json", true, true)
                        .AddJsonFile($"appsettings.{hostingContext.HostingEnvironment.
→EnvironmentName}.json", true, true)
                        .AddJsonFile("ocelot.json")
                        .AddEnvironmentVariables();
                })
        }
    }
}

```

(continues on next page)

<sup>1</sup> The `AddOcelot` method adds default ASP.NET services to DI-container. You could call another more extended `AddOcelotUsingBuilder` method while configuring services to build and use custom builder via an `IMvcCoreBuilder` interface object. See more instructions in [Dependency Injection](#), “The `AddOcelotUsingBuilder` method” section.

(continued from previous page)

```
.ConfigureServices(s => {
    s.AddOcelot();
})
.ConfigureLogging((hostingContext, logging) =>
{
    //add your logging
})
.UseIISIntegration()
.Configure(app =>
{
    app.UseOcelot().Wait();
})
.Build()
.Run();
}
}
```





## CONTRIBUTING

Pull requests, issues and commentary welcome!

Ideas, questions could be posted to Ocelot [Discussions](#) space.

We do follow development process which is described in [Release Process](#).



## NOT SUPPORTED

Ocelot does not support...

### 4.1 Chunked Encoding

Ocelot will always get the body size and return `Content-Length` header. Sorry, if this doesn't work for your use case!

### 4.2 Forwarding a Host header

The `Host` header that you send to Ocelot will not be forwarded to the downstream service. Obviously this would break everything

### 4.3 Swagger

Contributors have looked multiple times at building `swagger.json` out of the Ocelot `ocelot.json` but it doesn't fit into the vision the team has for Ocelot. If you would like to have Swagger in Ocelot then you must roll your own `swagger.json` and do the following in your `Startup.cs` or `Program.cs`. The code sample below registers a piece of middleware that loads your hand rolled `swagger.json` and returns it on `/swagger/v1/swagger.json`. It then registers the SwaggerUI middleware from `Swashbuckle.AspNetCore` package:

```
app.Map("/swagger/v1/swagger.json", b =>
{
    b.Run(async x => {
        var json = File.ReadAllText("swagger.json");
        await x.Response.WriteAsync(json);
    });
});
app.UseSwaggerUI(c =>
{
    c.SwaggerEndpoint("/swagger/v1/swagger.json", "Ocelot");
});

app.UseOcelot().Wait();
```

The main reasons why we don't think Swagger makes sense is we already hand roll our definition in `ocelot.json`. If we want people developing against Ocelot to be able to see what routes are available then either share the `ocelot.json` with

them (This should be as easy as granting access to a repo etc) or use the Ocelot [Administration](#) API so that they can query Ocelot for the configuration.

In addition to this, many people will configure Ocelot to proxy all traffic like `/products/{everything}` to their product service and you would not be describing what is actually available if you parsed this and turned it into a Swagger path. Also Ocelot has no concept of the models that the downstream services can return and linking to the above problem the same endpoint can return multiple models. Ocelot does not know what models might be used in POST, PUT etc, so it all gets a bit messy, and finally, the Swashbuckle package doesn't reload **swagger.json** if it changes during runtime. Ocelot's configuration can change during runtime so the Swagger and Ocelot information would not match. Unless we rolled our own Swagger implementation.

If the developer wants something to easily test against the Ocelot API then we suggest using [Postman](#) as a simple way to do this. It might even be possible to write something that maps **ocelot.json** to the Postman JSON spec. However we don't intend to do this.

**GOTCHAS**

## 5.1 IIS

Microsoft Learn: [Host ASP.NET Core on Windows with IIS](#)

We do not recommend to deploy Ocelot app to IIS environments, but if you do, keep in mind the gotchas below.

- When using ASP.NET Core 2.2+ and you want to use In-Process hosting, replace `UseIISIntegration()` with `UseIIS()`, otherwise you will get startup errors.
- Make sure you use Out-of-process hosting model instead of In-process one (see [Out-of-process hosting with IIS and ASP.NET Core](#)), otherwise you will get very slow responses (see [1657](#)).
- Ensure all DNS servers of all downstream hosts are online and they function perfectly, otherwise you will get slow responses (see [1630](#)).

The community constantly reports [issues related to IIS](#). If you have some troubles in IIS environment to host Ocelot app, first of all, read open/closed issues, and after that, search for [IIS](#) in the repository. Probably you will find a ready solution by Ocelot community members.

Finally, we have special label [for all IIS related objects](#). Feel free to put this label onto issues, PRs, discussions, etc.



## ADMINISTRATION

Ocelot supports changing configuration during runtime via an authenticated HTTP API. This can be authenticated in two ways either using Ocelot's internal IdentityServer (for authenticating requests to the administration API only) or hooking the administration API authentication into your own IdentityServer.

The first thing you need to do if you want to use the administration API is bring in the relevant [NuGet package](#):

```
Install-Package Ocelot.Administration
```

This will bring down everything needed by the administration API.

### 6.1 Providing your own IdentityServer

All you need to do to hook into your own IdentityServer is add the following configuration options with authentication to your `ConfigureServices` method. After that we must pass these options to `AddAdministration()` extension of the `OcelotBuilder` being returned by `AddOcelot()`<sup>1</sup> like below:

```
public virtual void ConfigureServices(IServiceCollection services)
{
    Action<JwtBearerOptions> options = o =>
    {
        o.Authority = identityServerRootUrl;
        o.RequireHttpsMetadata = false;
        o.TokenValidationParameters = new TokenValidationParameters
        {
            ValidateAudience = false,
        };
        // etc...
    };

    services
        .AddOcelot()
        .AddAdministration("/administration", options);
}
```

You now need to get a token from your IdentityServer and use in subsequent requests to Ocelot's administration API.

---

<sup>1</sup> The `AddOcelot` method adds default ASP.NET services to DI-container. You could call another more extended `AddOcelotUsingBuilder` method while configuring services to build and use custom builder via an `IMvcCoreBuilder` interface object. See more instructions in [Dependency Injection](#), "The `AddOcelotUsingBuilder` method" section.

This feature was implemented for [Issue 228](#). It is useful because the IdentityServer authentication middleware needs the URL of the IdentityServer. If you are using the internal IdentityServer, it might not always be possible to have the Ocelot URL.

## 6.2 Internal IdentityServer

The API is authenticated using Bearer tokens that you request from Ocelot itself. This is provided by the amazing [Identity Server](#) project that the .NET community has been using for several years. Check them out.

In order to enable the administration section, you need to do a few things. First of all, add this to your initial **Startup.cs**.

The path can be anything you want and it is obviously recommended don't use a URL you would like to route through with Ocelot as this will not work. The administration uses the `MapWhen` functionality of ASP.NET Core and all requests to `"{root}/administration"` will be sent there not to the Ocelot middleware.

The secret is the client secret that Ocelot's internal IdentityServer will use to authenticate requests to the administration API. This can be whatever you want it to be! In order to pass this secret string as parameter, we must call the `AddAdministration()` extension of the `OcelotBuilder` being returned by `AddOcelot()` [Page 17, 1](#) like below:

```
public virtual void ConfigureServices(IServiceCollection services)
{
    services
        .AddOcelot()
        .AddAdministration("/administration", "secret");
}
```

In order for the administration API to work, Ocelot / IdentityServer must be able to call itself for validation. This means that you need to add the base URL of Ocelot to global configuration if it is not default `http://localhost:5000`. Please note, if you are using something like Docker to host Ocelot it might not be able to call back to **localhost** etc, and you need to know what you are doing with Docker networking in this scenario. Anyway, this can be done as follows.

If you want to run on a different host and port locally:

```
"GlobalConfiguration": {
  "BaseUrl": "http://localhost:55580"
}
```

or if Ocelot is exposed via DNS:

```
"GlobalConfiguration": {
  "BaseUrl": "http://mydns.com"
}
```

Now, if you went with the configuration options above and want to access the API, you can use the Postman scripts called **ocelot.postman\_collection.json** in the solution to change the Ocelot configuration. Obviously these will need to be changed if you are running Ocelot on a different URL to `http://localhost:5000`.

The scripts show you how to request a Bearer token from Ocelot and then use it to GET the existing configuration and POST a configuration.

If you are running multiple Ocelot instances in a cluster then you need to use a certificate to sign the Bearer tokens used to access the administration API.

In order to do this, you need to add two more environmental variables for each Ocelot in the cluster:

1. **OCELOT\_CERTIFICATE** The path to a certificate that can be used to sign the tokens. The certificate needs to be of the type X509 and obviously Ocelot needs to be able to access it.



2. `OCELOT_CERTIFICATE_PASSWORD` The password for the certificate.

Normally Ocelot just uses temporary signing credentials but if you set these environmental variables then it will use the certificate. If all the other Ocelot instances in the cluster have the same certificate then you are good!

## 6.3 Administration API

### 6.3.1 POST {adminPath}/connect/token

This gets a token for use with the admin area using the client credentials we talk about setting above. Under the hood this calls into an IdentityServer hosted within Ocelot.

The body of the request is form-data as follows:

- `client_id` set as admin
- `client_secret` set as whatever you used when setting up the administration services.
- `scope` set as admin
- `grant_type` set as client\_credentials

### 6.3.2 GET {adminPath}/configuration

This gets the current Ocelot configuration. It is exactly the same JSON we use to set Ocelot up with in the first place.

### 6.3.3 POST {adminPath}/configuration

This overwrites the existing configuration (should probably be a PUT!). We recommend getting your config from the GET endpoint, making any changes and posting it back... simples.

The body of the request is JSON and it is the same format as the [FileConfiguration](#) that we use to set up Ocelot on a file system.

Please note, if you want to use this API then the process running Ocelot must have permission to write to the disk where your `ocelot.json` or `ocelot.{environment}.json` is located. This is because Ocelot will overwrite them on save.

### 6.3.4 DELETE {adminPath}/outputcache/{region}

This clears a region of the cache. If you are using a backplane, it will clear all instances of the cache! Giving your the ability to run a cluster of Ocelots and cache over all of them in memory and clear them all at the same time, so just use a distributed cache.

The region is whatever you set against the **Region** field in the [FileCacheOptions](#) section of the Ocelot configuration.

---



## **AUTHENTICATION**

In order to authenticate Routes and subsequently use any of Ocelot's claims based features such as authorization or modifying the request with values from the token, users must register authentication services in their **Startup.cs** as usual but they provide a scheme (authentication provider key) with each registration e.g.

```
public void ConfigureServices(IServiceCollection services)
{
    var authenticationProviderKey = "TestKey";
    services
        .AddAuthentication()
        .AddJwtBearer(authenticationProviderKey,
            options => { /* custom auth-setup */ });
}
```

In this example “**TestKey**” is the scheme that this provider has been registered with. We then map this to a Route in the configuration e.g.

```
"Routes": [{
  "AuthenticationOptions": {
    "AuthenticationProviderKey": "TestKey",
    "AllowedScopes": []
  }
}]
```

When Ocelot runs it will look at this `Routes.AuthenticationOptions.AuthenticationProviderKey` and check that there is an authentication provider registered with the given key. If there isn't then Ocelot will not start up. If there is then the Route will use that provider when it executes.

If a Route is authenticated, Ocelot will invoke whatever scheme is associated with it while executing the authentication middleware. If the request fails authentication, Ocelot returns a HTTP status code **401 Unauthorized**.

### **7.1 JWT Tokens**

If you want to authenticate using JWT tokens maybe from a provider like [Auth0](#), you can register your authentication middleware as normal e.g.

```
public void ConfigureServices(IServiceCollection services)
{
    var authenticationProviderKey = "TestKey";
    services
        .AddAuthentication()
```

(continues on next page)

(continued from previous page)

```
.AddJwtBearer(authenticationProviderKey, options =>
{
    options.Authority = "test";
    options.Audience = "test";
});
services.AddOcelot();
}
```

Then map the authentication provider key to a Route in your configuration e.g.

```
"Routes": [{
  "AuthenticationOptions": {
    "AuthenticationProviderKey": "TestKey",
    "AllowedScopes": []
  }
}]
```

## 7.2 Identity Server Bearer Tokens

In order to use [IdentityServer](#) bearer tokens, register your IdentityServer services as usual in `ConfigureServices` with a scheme (key). If you don't understand how to do this, please consult the [IdentityServer documentation](#).

```
public void ConfigureServices(IServiceCollection services)
{
    var authenticationProviderKey = "TestKey";
    Action<JwtBearerOptions> options = (opt) =>
    {
        opt.Authority = "https://whereyouridentityserverlives.com";
        // ...
    };
    services
        .AddAuthentication()
        .AddJwtBearer(authenticationProviderKey, options);
    services.AddOcelot();
}
```

Then map the authentication provider key to a Route in your configuration e.g.

```
"Routes": [{
  "AuthenticationOptions": {
    "AuthenticationProviderKey": "TestKey",
    "AllowedScopes": []
  }
}]
```

## 7.3 Auth0 by Okta

Yet another identity provider by [Okta](#), see [Auth0 Developer Resources](#).

Add the following to your startup `Configure` method:

```
app.UseAuthentication()
    .UseOcelot().Wait();
```

Add the following, at minimum, to your startup `ConfigureServices` method:

```
services
    .AddAuthentication()
    .AddJwtBearer(oktaProviderKey, options =>
    {
        options.Audience = configuration["Authentication:Okta:Audience"]; // Okta_
        ↪ Authorization server Audience
        options.Authority = configuration["Authentication:Okta:Server"]; // Okta_
        ↪ Authorization Issuer URI URL e.g. https://{subdomain}.okta.com/oauth2/{authidentifier}
    });
services.AddOcelot(configuration);
```

**Note** In order to get Ocelot to view the scope claim from Okta properly, you have to add the following to map the default Okta "scp" claim to "scope":

```
// Map Okta "scp" to "scope" claims instead of http://schemas.microsoft.com/identity/
↪ claims/scope to allow Ocelot to read/verify them
JwtSecurityTokenHandler.DefaultInboundClaimTypeMap.Remove("scp");
JwtSecurityTokenHandler.DefaultInboundClaimTypeMap.Add("scp", "scope");
```

[Issue 446](#) contains some code and examples that might help with Okta integration.

## 7.4 Allowed Scopes

If you add scopes to **AllowedScopes**, Ocelot will get all the user claims (from the token) of the type scope and make sure that the user has at least one of the scopes in the list.

This is a way to restrict access to a Route on a per scope basis.

## 7.5 More identity providers

We invite you to add more examples, if you have integrated with other identity providers and the integration solution is working. Please, open [Show and tell](#) discussion in the repository.



## AUTHORIZATION

Ocelot supports claims based authorization which is run post authentication. This means if you have a route you want to authorize, you can add the following to your Route configuration:

```
"RouteClaimsRequirement": {  
  "UserType": "registered"  
}
```

In this example, when the `AuthorizationMiddleware` is called, Ocelot will check to see if the user has the claim type `UserType` and if the value of that claim is "registered". If it isn't then the user will not be authorized and the response will be 403 `Forbidden`.

### 8.1 Authorization Middleware

The `AuthorizationMiddleware` is built-in into Ocelot pipeline.

Previous private: `ClaimsToClaimsMiddleware`

Previous public: `PreAuthorizationMiddleware`

**This:** `AuthorizationMiddleware`

Next private: `ClaimsToHeadersMiddleware`

Next public: `PreQueryStringBuilderMiddleware`

So, the closest middlewares are in order of calling:

<code>ClaimsToClaimsMiddleware</code>	<code>PreAuthorizationMiddleware</code>	<b><code>AuthorizationMiddleware</code></b>
<code>ClaimsToHeadersMiddleware</code>	<code>PreQueryStringBuilderMiddleware</code>	

As you may know from the *Middleware Injection* section, the `Authorization` middleware can be overridden like this:

```
public void Configure(IApplicationBuilder app, IWebHostEnvironment env)  
{  
    var configuration = new OcelotPipelineConfiguration  
    {  
        AuthorizationMiddleware = async (context, next) =>  
        {  
            await next.Invoke();  
        }  
    };  
    app.UseOcelot(configuration);  
}
```

Do this in very rare cases, because overriding Authorization middleware means you will lose claims & scopes authorizer through the **RouteClaimsRequirement** property of the route. Another option is preparing before the actual authorization in `PreAuthorizationMiddleware` which is public and open to overriding.



## CACHING

Ocelot supports some very rudimentary caching at the moment provided by the [CacheManager](#) project. This is an amazing project that is solving a lot of caching problems. We would recommend using this package to cache with Ocelot.

The following example shows how to add **CacheManager** to Ocelot so that you can do output caching.

First of all, add the following [NuGet package](#):

```
Install-Package Ocelot.Cache.CacheManager
```

This will give you access to the Ocelot cache manager extension methods.

The second thing you need to do something like the following to your `ConfigureServices` method:

```
using Ocelot.Cache.CacheManager;

ConfigureServices(services =>
{
    services.AddOcelot()
        .AddCacheManager(x => x.WithDictionaryHandle());
});
```

Finally, in order to use caching on a route in your Route configuration add this setting:

```
"FileCacheOptions": { "TtlSeconds": 15, "Region": "somename" }
```

In this example **TtlSeconds** is set to 15 which means the cache will expire after 15 seconds. The **Region** represents a region of caching.

If you look at the example [here](#) you can see how the cache manager is setup and then passed into the Ocelot `AddCacheManager` configuration method. You can use any settings supported by the **CacheManager** package and just pass them in.

Anyway, Ocelot currently supports caching on the URL of the downstream service and setting a TTL in seconds to expire the cache. You can also clear the cache for a region by calling Ocelot's administration API.

## 9.1 Your Own Caching

If you want to add your own caching method, implement the following interfaces and register them in DI e.g.

```
services.AddSingleton<IOcelotCache<CachedResponse>, MyCache>();
```

- `IOcelotCache<CachedResponse>` this is for output caching.
- `IOcelotCache<FileConfiguration>` this is for caching the file configuration if you are calling something remote to get your config such as Consul.

Please dig into the Ocelot source code to find more. We would really appreciate it if anyone wants to implement [Redis](#), [Memcached](#) etc. Please, open a new [Show and tell](#) thread in [Discussions](#) space of the repository.

## CLAIMS TRANSFORMATION

Ocelot allows the user to access claims and transform them into headers, query string parameters, other claims and change downstream paths. This is only available once a user has been authenticated.

After the user is authenticated, we run the claims to claims transformation middleware (see the [ClaimsToClaimsMiddleware](#) class). This allows the user to transform claims before the authorization middleware is called. After the user is authorized, we call the claims to headers middleware (see the [ClaimsToHeadersMiddleware](#) class), then the claims to query string parameters middleware (see the [ClaimsToQueryStringMiddleware](#) class), and finally the claims to downstream path middleware (see the [ClaimsToDownstreamPathMiddleware](#) class).

The syntax for performing the transforms is the same for each process. In the Route configuration, a JSON dictionary is added with a specific name either **AddClaimsToRequest**, **AddHeadersToRequest**, **AddQueriesToRequest**, or **ChangeDownstreamPathTemplate**.

Note: This syntax is not ideal. So any suggestions are welcome...

Within this dictionary the entries specify how Ocelot should transform things! The key to the dictionary is going to become the key of either a claim, header or query parameter. In the case of **ChangeDownstreamPathTemplate**, the key must be also specified in the **DownstreamPathTemplate**, in order to do the transformation.

The value of the entry is parsed to logic that will perform the transform. First of all, a dictionary accessor is specified e.g. `Claims[CustomerId]`. This means we want to access the claims and get the `CustomerId` claim type. Next is a “greater than” `>` symbol which is just used to split the string. The next entry is either value or value with an indexer. If value is specified, Ocelot will just take the value and add it to the transform. If the value has an indexer, Ocelot will look for a delimiter which is provided after another “greater than” `>` symbol. Ocelot will then split the value on the delimiter and add whatever was at the index requested to the transform.

### 10.1 Claims to Claims Transformation

Below is an example configuration that will transform claims to claims

```
"AddClaimsToRequest": {  
  "UserType": "Claims[sub] > value[0] > |",  
  "UserId": "Claims[sub] > value[1] > |"  
}
```

This shows a transforms where Ocelot looks at the users `sub` claim and transforms it into **UserType** and **UserId** claims. Assuming the `sub` looks like this `usertypevalue|useridvalue`.

## 10.2 Claims to Headers Transformation

Below is an example configuration that will transform claims to headers

```
"AddHeadersToRequest": {  
  "CustomerId": "Claims[sub] > value[1] > |"  
}
```

This shows a transform where Ocelot looks at the users `sub` claim and transforms it into a **CustomerId** header. Assuming the `sub` looks like this `usertypevalue|useridvalue`.

## 10.3 Claims to Query String Parameters Transformation

Below is an example configuration that will transform claims to query string parameters

```
"AddQueriesToRequest": {  
  "LocationId": "Claims[LocationId] > value",  
}
```

This shows a transform where Ocelot looks at the users `LocationId` claim and add it as a query string parameter to be forwarded onto the downstream service.

## 10.4 Claims to Downstream Path Transformation

Below is an example configuration that will transform claims to downstream path custom placeholders:

```
"UpstreamPathTemplate": "/api/users/me/{everything}",  
"DownstreamPathTemplate": "/api/users/{userId}/{everything}",  
"ChangeDownstreamPathTemplate": {  
  "userId": "Claims[sub] > value[1] > |",  
}
```

This shows a transform where Ocelot looks at the users `userId` claim and substitutes the value to the “{userId}” placeholder specified in the **DownstreamPathTemplate**. Take into account that the key specified in the **ChangeDownstreamPathTemplate** must be the same than the placeholder specified in the **DownstreamPathTemplate**.

Note: If a key specified in the **ChangeDownstreamPathTemplate** does not exist as a placeholder in **DownstreamPathTemplate**, it will fail at runtime returning an error in the response.

## CONFIGURATION

An example configuration can be found here in [ocelot.json](#). There are two sections to the configuration: an array of **Routes** and a **GlobalConfiguration**:

- The **Routes** are the objects that tell Ocelot how to treat an upstream request.
- The **GlobalConfiguration** is a bit hacky and allows overrides of Route specific settings. It's useful if you do not want to manage lots of Route specific settings.

```
{  
  "Routes": [],  
  "GlobalConfiguration": {}  
}
```

Here is an example Route configuration. You don't need to set all of these things but this is everything that is available at the moment:

```
{  
  "DownstreamPathTemplate": "/",  
  "UpstreamPathTemplate": "/",  
  "UpstreamHttpMethod": [ "Get" ],  
  "DownstreamHttpMethod": "",  
  "DownstreamHttpVersion": "",  
  "AddHeadersToRequest": {},  
  "AddClaimsToRequest": {},  
  "RouteClaimsRequirement": {},  
  "AddQueriesToRequest": {},  
  "RequestIdKey": "",  
  "FileCacheOptions": {  
    "TtlSeconds": 0,  
    "Region": "europe-central"  
  },  
  "RouteIsCaseSensitive": false,  
  "ServiceName": "",  
  "DownstreamScheme": "http",  
  "DownstreamHostAndPorts": [  
    { "Host": "localhost", "Port": 51876 }  
  ],  
  "QoSOptions": {  
    "ExceptionsAllowedBeforeBreaking": 0,  
    "DurationOfBreak": 0,  
    "TimeoutValue": 0  
  },  
}
```

(continues on next page)

(continued from previous page)

```

"LoadBalancer": "",
"RateLimitOptions": {
  "ClientWhitelist": [],
  "EnableRateLimiting": false,
  "Period": "",
  "PeriodTimespan": 0,
  "Limit": 0
},
"AuthenticationOptions": {
  "AuthenticationProviderKey": "",
  "AllowedScopes": []
},
"HttpHandlerOptions": {
  "AllowAutoRedirect": true,
  "UseCookieContainer": true,
  "UseTracing": true,
  "MaxConnectionsPerServer": 100
},
"DangerousAcceptAnyServerCertificateValidator": false,
"SecurityOptions": {
  "IPAllowedList": [],
  "IPBlockedList": [],
  "ExcludeAllowedFromBlocked": false
}
}

```

More information on how to use these options is below.

## 11.1 Multiple Environments

Like any other ASP.NET Core project Ocelot supports configuration file names such as **configuration.dev.json**, **configuration.test.json** etc. In order to implement this add the following to you:

```

ConfigureAppConfiguration((hostingContext, config) =>
{
    config
        .SetBasePath(hostingContext.HostingEnvironment.ContentRootPath)
        .AddJsonFile("appsettings.json", true, true)
        .AddJsonFile($"appsettings.{hostingContext.HostingEnvironment.EnvironmentName}.
↪json", true, true)
        .AddJsonFile("ocelot.json")
        .AddJsonFile($"configuration.{hostingContext.HostingEnvironment.EnvironmentName}.
↪json")
        .AddEnvironmentVariables();
})

```

Ocelot will now use the environment specific configuration and fall back to **ocelot.json** if there isn't one.

You also need to set the corresponding environment variable which is `ASPNETCORE_ENVIRONMENT`. More info on this can be found in the ASP.NET Core docs: [Use multiple environments in ASP.NET Core](#).

## 11.2 Merging Configuration Files

This feature was requested in [issue 296](#) and allows users to have multiple configuration files to make managing large configurations easier.

Instead of adding the configuration directly e.g. `AddJsonFile("ocelot.json")` you can call `AddOcelot()` like below:

```
ConfigureAppConfiguration((hostingContext, config) =>
{
    config
        .SetBasePath(hostingContext.HostingEnvironment.ContentRootPath)
        .AddJsonFile("appsettings.json", true, true)
        .AddJsonFile($"appsettings.{hostingContext.HostingEnvironment.EnvironmentName}.
↪json", true, true)
        .AddOcelot(hostingContext.HostingEnvironment)
        .AddEnvironmentVariables();
})
```

In this scenario Ocelot will look for any files that match the pattern `(?i)ocelot.([a-zA-Z0-9]*)\.json` and then merge these together. If you want to set the **GlobalConfiguration** property, you must have a file called **ocelot.global.json**.

The way Ocelot merges the files is basically load them, loop over them, add any Routes, add any **AggregateRoutes** and if the file is called **ocelot.global.json** add the **GlobalConfiguration** as well as any Routes or **AggregateRoutes**. Ocelot will then save the merged configuration to a file called **ocelot.json** and this will be used as the source of truth while Ocelot is running.

At the moment there is no validation at this stage it only happens when Ocelot validates the final merged configuration. This is something to be aware of when you are investigating problems. We would advise always checking what is in **ocelot.json** file if you have any problems.

You can also give Ocelot a specific path to look in for the configuration files like below:

```
ConfigureAppConfiguration((hostingContext, config) =>
{
    config
        .SetBasePath(hostingContext.HostingEnvironment.ContentRootPath)
        .AddJsonFile("appsettings.json", true, true)
        .AddJsonFile($"appsettings.{hostingContext.HostingEnvironment.EnvironmentName}.
↪json", true, true)
        .AddOcelot("/foo/bar", hostingContext.HostingEnvironment)
        .AddEnvironmentVariables();
})
```

Ocelot needs the `HostingEnvironment` so it knows to exclude anything environment specific from the algorithm.

## 11.3 Store Configuration in Consul

The first thing you need to do is install the [NuGet package](#) that provides [Consul](#) support in Ocelot.

```
Install-Package Ocelot.Provider.Consul
```

Then you add the following when you register your services Ocelot will attempt to store and retrieve its configuration in Consul KV store. In order to register Consul services we must call the `AddConsul()` and `AddConfigStoredInConsul()` extensions using the `OcelotBuilder` being returned by `AddOcelot()`<sup>1</sup> like below:

```
services
    .AddOcelot()
    .AddConsul()
    .AddConfigStoredInConsul();
```

You also need to add the following to your **ocelot.json**. This is how Ocelot finds your Consul agent and interacts to load and store the configuration from Consul.

```
"GlobalConfiguration": {
  "ServiceDiscoveryProvider": {
    "Host": "localhost",
    "Port": 9500
  }
}
```

The team decided to create this feature after working on the Raft consensus algorithm and finding out its super hard. Why not take advantage of the fact Consul already gives you this! We guess it means if you want to use Ocelot to its fullest, you take on Consul as a dependency for now.

This feature has a 3 seconds TTL cache before making a new request to your local Consul agent.

## 11.4 Reload JSON Config On Change

Ocelot supports reloading the JSON configuration file on change. For instance, the following will recreate Ocelot internal configuration when the **ocelot.json** file is updated manually:

```
config.AddJsonFile("ocelot.json", optional: false, reloadOnChange: true);
```

## 11.5 Configuration Key

If you are using Consul for configuration (or other providers in the future), you might want to key your configurations: so you can have multiple configurations. This feature was requested in [issue 346](#). In order to specify the key you need to set the **ConfigurationKey** property in the **ServiceDiscoveryProvider** options of the configuration JSON file e.g.

```
"GlobalConfiguration": {
  "ServiceDiscoveryProvider": {
    "Host": "localhost",
```

(continues on next page)

<sup>1</sup> The `AddOcelot` method adds default ASP.NET services to DI-container. You could call another more extended `AddOcelotUsingBuilder` method while configuring services to build and use custom builder via an `IMvcCoreBuilder` interface object. See more instructions in [Dependency Injection](#), “The `AddOcelotUsingBuilder` method” section.



(continued from previous page)

```

    "Port": 9500,
    "ConfigurationKey": "Ocelot_A"
  }
}

```

In this example Ocelot will use `Ocelot_A` as the key for your configuration when looking it up in Consul. If you do not set the **ConfigurationKey**, Ocelot will use the string `InternalConfiguration` as the key.

## 11.6 Follow Redirects aka `HttpHandlerOptions`

Class: `FileHttpHandlerOptions`

Use `HttpHandlerOptions` in a Route configuration to set up `HttpHandler` behavior:

```

"HttpHandlerOptions": {
  "AllowAutoRedirect": false,
  "UseCookieContainer": false,
  "UseTracing": true,
  "MaxConnectionsPerServer": 100
},

```

- **AllowAutoRedirect** is a value that indicates whether the request should follow redirection responses. Set it `true` if the request should automatically follow redirection responses from the downstream resource; otherwise `false`. The default value is `false`.
- **UseCookieContainer** is a value that indicates whether the handler uses the `CookieContainer` property to store server cookies and uses these cookies when sending requests. The default value is `false`. Please note, if you use the `CookieContainer`, Ocelot caches the `HttpClient` for each downstream service. This means that all requests to that downstream service will share the same cookies. [Issue 274](#) was created because a user noticed that the cookies were being shared. The Ocelot team tried to think of a nice way to handle this but we think it is impossible. If you don't cache the clients, that means each request gets a new client and therefore a new cookie container. If you clear the cookies from the cached client container, you get race conditions due to inflight requests. This would also mean that subsequent requests don't use the cookies from the previous response! All in all not a great situation. We would avoid setting **UseCookieContainer** to `true` unless you have a really really good reason. Just look at your response headers and forward the cookies back with your next request!
- **MaxConnectionsPerServer** This controls how many connections the internal `HttpClient` will open. This can be set at Route or global level.

## 11.7 SSL Errors

If you want to ignore SSL warnings (errors), set the following in your Route config:

```

"DangerousAcceptAnyServerCertificateValidator": true

```

**We don't recommend doing this!** The team suggests creating your own certificate and then getting it trusted by your local (remote) machine, if you can. For `https` scheme this fake validator was requested by [issue 309](#). For `wss` scheme this fake validator was added by [PR 1377](#).

As a team, we do not consider it as an ideal solution. From one side, the community wants to have an option to work with self-signed certificates. But from other side, currently source code scanners detect 2 serious security vulnerabilities

because of this fake validator in [20.0 release](#). The Ocelot team will rethink this unfortunate situation, and it is highly likely that this feature will at least be redesigned or removed completely.

For now, the SSL fake validator makes sense in local development environments when a route has `https` or `wss` schemes having self-signed certificate for those routes. There are no other reasons to use the **DangerousAcceptAnyServerCertificateValidator** property at all!

As a team, we highly recommend following these instructions when developing your gateway app with Ocelot:

- **Local development environments.** Use the feature to avoid SSL errors for self-signed certificates in case of `https` or `wss` schemes. We understand that some routes should have downstream scheme exactly with SSL, because they are also in development, and/or deployed using SSL protocols. But we believe that especially for local development, you can switch from `https` to `http` without any objection since the services are in development and there is no risk of data leakage.
- **Remote development environments.** Everything is the same as for local development. But this case is less strict, you have more options to use real certificates to switch off the feature. For instance, you can deploy downstream services to cloud & hosting providers which have own signed certificates for SSL. At least your team can deploy one remote web server to host downstream services. Install own certificate or use cloud provider's one.
- **Staging or testing environments.** We do not recommend to use self-signed certificates because web servers should have valid certificates installed. Ask your system administrator or DevOps engineers of your team to create valid certificates.
- **Production environments. Do not use self-signed certificates at all!** System administrators or DevOps engineers must create real valid certificates being signed by hosting or cloud providers. **Switch off the feature for all routes!** Remove the **DangerousAcceptAnyServerCertificateValidator** property for all routes in production version of **ocelot.json** file!

## 11.8 React to Configuration Changes

Resolve `IOcelotConfigurationChangeTokenSource` interface from the DI container if you wish to react to changes to the Ocelot configuration via the [Administration](#) API or **ocelot.json** being reloaded from the disk. You may either poll the change token's `ICancellationToken.HasChanged` property, or register a callback with the `RegisterChangeCallback` method.

### 11.8.1 Polling the HasChanged property

```
public class ConfigurationNotifyingService : BackgroundService
{
    private readonly IOcelotConfigurationChangeTokenSource _tokenSource;
    private readonly ILogger _logger;

    public ConfigurationNotifyingService(IOcelotConfigurationChangeTokenSource
↪tokenSource, ILogger logger)
    {
        _tokenSource = tokenSource;
        _logger = logger;
    }

    protected override async Task ExecuteAsync(CancellationToken stoppingToken)
    {
        while (!stoppingToken.IsCancellationRequested)

```

(continues on next page)

(continued from previous page)

```

    {
        if (_tokenSource.ChangeToken.HasChanged)
        {
            _logger.LogInformation("Configuration updated");
        }
        await Task.Delay(1000, stoppingToken);
    }
}

```

## 11.8.2 Registering a callback

```

public class MyDependencyInjectedClass : IDisposable
{
    private readonly IOcelotConfigurationChangeTokenSource _tokenSource;
    private readonly IDisposable _callbackHolder;

    public MyClass(IOcelotConfigurationChangeTokenSource tokenSource)
    {
        _tokenSource = tokenSource;
        _callbackHolder = tokenSource.ChangeToken.RegisterChangeCallback(_ => Console.
↪WriteLine("Configuration changed"), null);
    }
    public void Dispose()
    {
        _callbackHolder.Dispose();
    }
}

```

## 11.9 DownstreamHttpVersion

Ocelot allows you to choose the HTTP version it will use to make the proxy request. It can be set as 1.0, 1.1 or 2.0.



## DELEGATING HANDLERS

Ocelot allows the user to add delegating handlers to the `HttpClient` transport. This feature was requested by [issue 208](#) and the team decided that it was going to be useful in various ways. Since then we extended it in [issue 264](#).

### 12.1 How to Use

In order to add delegating handlers to the `HttpClient` transport you need to do two main things.

**First**, in order to create a class that can be used a delegating handler it must look as follows. We are going to register these handlers in the ASP.NET Core DI container, so you can inject any other services you have registered into the constructor of your handler.

```
public class FakeHandler : DelegatingHandler
{
    protected override async Task<HttpResponseMessage> SendAsync(HttpRequestMessage request, CancellationToken token)
    {
        // Do stuff and optionally call the base handler...
        return await base.SendAsync(request, token);
    }
}
```

**Second**, you must add the handlers to DI container like below:

```
ConfigureServices(s => s
    .AddOcelot()
    .AddDelegatingHandler<FakeHandler>()
    .AddDelegatingHandler<FakeHandlerTwo>()
)
```

Both of these `AddDelegatingHandler` methods have a default parameter called `global` which is set to `false`. If it is `false` then the intent of the *Delegating Handler* is to be applied to specific Routes via **ocelot.json** (more on that later). If it is set to `true` then it becomes a global handler and will be applied to all Routes, as below:

```
services.AddOcelot()
    .AddDelegatingHandler<FakeHandler>(true)
```

**Finally**, if you want Route specific *Delegating Handlers* or to order your specific and (or) global (more on this later) *Delegating Handlers* then you must add the following to the specific Route in **ocelot.json**. The names in the array must match the class names of your *Delegating Handlers* for Ocelot to match them together:

```
"DelegatingHandlers": [  
  "FakeHandlerTwo",  
  "FakeHandler"  
]
```

## 12.2 Order of Execution

You can have as many *Delegating Handlers* as you want and they are run in the following order:

1. Any globals that are left in the order they were added to services and are not in the **DelegatingHandlers** array from **ocelot.json**.
2. Any non global *Delegating Handlers* plus any globals that were in the **DelegatingHandlers** array from **ocelot.json** ordered as they are in the **DelegatingHandlers** array.
3. Tracing *Delegating Handler*, if enabled (see [Tracing](#) docs).
4. Quality of Service *Delegating Handler*, if enabled (see [Quality of Service](#) docs).
5. The **HttpClient** sends the **HttpRequestMessage**.

Hopefully other people will find this feature useful!

## DEPENDENCY INJECTION

**Namespace:** `Ocelot.DependencyInjection`

**Source code:** `DependencyInjection`

### 13.1 Overview

Dependency Injection feature in Ocelot is designed to extend and/or control building of Ocelot core as ASP.NET MVC pipeline services. The main methods are [AddOcelot](#) and [AddOcelotUsingBuilder](#) of the `ServiceCollectionExtensions` class. Use them in **Program.cs** and **Startup.cs** of your ASP.NET MVC gateway app (minimal web app) to enable and build Ocelot pipeline.

And of course, the [OcelotBuilder](#) class is the core of Ocelot.

### 13.2 IServiceCollection extensions

**Class:** `Ocelot.DependencyInjection.ServiceCollectionExtensions`

Based on the current implementations for the `OcelotBuilder` class, the `AddOcelot` method adds default ASP.NET services to DI container. You could call another more extended `AddOcelotUsingBuilder` method while configuring services to build and use custom builder via an `IMvcCoreBuilder` interface object.

#### 13.2.1 The AddOcelot method

**Signatures:**

- `IOcelotBuilder AddOcelot(this IServiceCollection services)`
- `IOcelotBuilder AddOcelot(this IServiceCollection services, IConfiguration configuration)`

This `IServiceCollection` extension method adds default ASP.NET services and Ocelot application services with configuration injected implicitly or explicitly. Note! The method adds **default** ASP.NET services required for Ocelot core in the [AddDefaultAspNetServices](#) method which plays the role of default builder.

In this scenario, you do nothing except calling the `AddOcelot` method which has been mentioned in feature chapters, if additional startup settings are required. In this case you just reuse default settings to build Ocelot core. The alternative is `AddOcelotUsingBuilder` method, see the next section.

### 13.2.2 The AddOcelotUsingBuilder method

#### Signatures:

- `IOcelotBuilder AddOcelotUsingBuilder(this IServiceCollection services, Func<IMvcCoreBuilder, Assembly, IMvcCoreBuilder> customBuilder)`
- `IOcelotBuilder AddOcelotUsingBuilder(this IServiceCollection services, IConfiguration configuration, Func<IMvcCoreBuilder, Assembly, IMvcCoreBuilder> customBuilder)`

This `IServiceCollection` extension method adds Ocelot application services, and it *adds custom ASP.NET services* with configuration injected implicitly or explicitly. Note! The method adds **custom** ASP.NET services required for Ocelot pipeline using custom builder (`customBuilder` parameter). It is highly recommended to read docs of the [AddDefaultAspNetServices](#) method, or even to review implementation to understand default ASP.NET services which are the minimal part of the gateway pipeline.

In this custom scenario, you control everything during ASP.NET MVC pipeline building, and you provide custom settings to build Ocelot core.

## 13.3 The OcelotBuilder class

**Source code:** [Ocelot.DependencyInjection.OcelotBuilder](#)

The `OcelotBuilder` class is the core of Ocelot which does the following:

- Constructs itself by single public constructor: `public OcelotBuilder(IServiceCollection services, IConfiguration configurationRoot, Func<IMvcCoreBuilder, Assembly, IMvcCoreBuilder> customBuilder = null)`
- Initializes and stores public properties: **Services** (`IServiceCollection` object), **Configuration** (`IConfiguration` object) and **MvcCoreBuilder** (`IMvcCoreBuilder` object)
- Adds **all application services** during construction phase over the `Services` property
- Adds ASP.NET services by builder using `Func<IMvcCoreBuilder, Assembly, IMvcCoreBuilder>` object in these 2 development scenarios:
  - by default builder (`AddDefaultAspNetServices` method) if there is no `customBuilder` parameter provided
  - by custom builder with provided delegate object as the `customBuilder` parameter
- Adds (switches on/off) Ocelot features by:
  - `AddSingletonDefinedAggregator` and `AddTransientDefinedAggregator` methods
  - `AddCustomLoadBalancer` method
  - `AddDelegatingHandler` method
  - `AddConfigPlaceholders` method



### 13.3.1 The AddDefaultAspNetServices method

**Class:** `Ocelot.DependencyInjection.OcelotBuilder`

Currently the method is protected and overriding is forbidden. The role of the method is to inject required services via both `IServiceCollection` and `IMvcCoreBuilder` interfaces objects for the minimal part of the gateway pipeline.

Current implementation is the following:

```
protected IMvcCoreBuilder AddDefaultAspNetServices(IMvcCoreBuilder builder, Assembly
↪assembly)
{
    Services
        .AddLogging()
        .AddMiddlewareAnalysis()
        .AddWebEncoders();

    return builder
        .AddApplicationPart(assembly)
        .AddControllersAsServices()
        .AddAuthorization()
        .AddNewtonsoftJson();
}
```

The method cannot be overridden. It is not virtual, and there is no way to override current behavior by inheritance. And, the method is default builder of Ocelot pipeline while calling the [AddOcelot](#) method. As alternative, to “override” this default builder, you can design and reuse custom builder as a `Func<IMvcCoreBuilder, Assembly, IMvcCoreBuilder>` delegate object and pass it as parameter to the [AddOcelotUsingBuilder](#) extension method. It gives you full control on design and buiding of Ocelot pipeline, but be careful while designing your custom Ocelot pipeline as customizable ASP.NET MVC pipeline.

Warning! Most of services from minimal part of the pipeline should be reused, but only a few of services could be removed.

Warning!! The method above is called after adding required services of ASP.NET MVC pipeline building by [AddMvcCore](#) method over the `Services` property in upper calling context. These services are absolute minimum core services for ASP.NET MVC pipeline. They must be added to DI container always, and they are added implicitly before calling of the method by caller in upper context. So, `AddMvcCore` creates an `IMvcCoreBuilder` object with its assignment to the `MvcCoreBuilder` property. Finally, as a default builder, the method above receives `IMvcCoreBuilder` object being ready for further extensions.

The next section shows you an example of designing custom Ocelot pipeline by custom builder.

## 13.4 Custom Builder

**Goal:** Replace `Newtonsoft.Json` services with `System.Text.Json` services.

### 13.4.1 The Problem

The default `AddOcelot` method adds `Newtonsoft JSON` services by the `AddNewtonsoftJson` extension method in default builder (the `AddDefaultAspNetServices` method). The `AddNewtonsoftJson` method calling was introduced in old .NET and Ocelot releases which was necessary when Microsoft did not launch the `System.Text.Json` library, but now it affects normal use, so we have an intention to solve the problem.

Modern `JSON services` out of the box will help to configure JSON settings by the `JsonSerializerOptions` property for JSON formatters during (de)serialization.

### 13.4.2 Solution

We have the following methods in `Ocelot.DependencyInjection.ServiceCollectionExtensions` class:

- `IOcelotBuilder AddOcelotUsingBuilder(this IServiceCollection services, Func<IMvcCoreBuilder, Assembly, IMvcCoreBuilder> customBuilder)`
- `IOcelotBuilder AddOcelotUsingBuilder(this IServiceCollection services, IConfiguration configuration, Func<IMvcCoreBuilder, Assembly, IMvcCoreBuilder> customBuilder)`

These method with custom builder allows you to use your any desired JSON library for (de)serialization. But we are going to create custom `MvcCoreBuilder` with support of JSON services, such as `System.Text.Json`. To do that we need to call `AddJsonOptions` extension of the `MvcCoreMvcCoreBuilderExtensions` class (NuGet package: `Microsoft.AspNetCore.Mvc.Core`) in `Startup.cs`:

```
using Microsoft.Extensions.DependencyInjection;
using Ocelot.DependencyInjection;
using System.Reflection;

public class Startup
{
    public void ConfigureServices(IServiceCollection services)
    {
        services
            .AddLogging()
            .AddMiddlewareAnalysis()
            .AddWebEncoders()
            // Add your custom builder
            .AddOcelotUsingBuilder(MyCustomBuilder);
    }

    private static IMvcCoreBuilder MyCustomBuilder(IMvcCoreBuilder builder, Assembly
↪assembly)
    {
        return builder
            .AddApplicationPart(assembly)
            .AddControllersAsServices()
            .AddAuthorization()
    }
}
```

(continues on next page)

(continued from previous page)

```
// Replace AddNewtonsoftJson() by AddJsonOptions()
.AddJsonOptions(options =>
{
    options.JsonSerializerOptions.WriteIndented = true; // use System.Text.
})
}
}
```

The sample code provides settings to render JSON as indented text rather than compressed plain JSON text without spaces. This is just one common use case, and you can add additional services to the builder.



## ERROR STATUS CODES

Ocelot will return HTTP status error codes based on internal logic in certain situations:

### 14.1 Client error responses

- **401** - if the authentication middleware runs and the user is not authenticated.
- **403** - if the authorization middleware runs and the user is unauthenticated, claim value not authorized, scope not authorized, user doesn't have required claim, or cannot find claim.
- **404** - if unable to find a downstream route, or Ocelot is unable to map an internal error code to a HTTP status code.
- **499** - if the request is cancelled by the client.


### 14.2 Server error responses

- **500** - if unable to complete the HTTP request to downstream service, and the exception is not `OperationCanceledException` or `HttpRequestException`.
- **502** - if unable to connect to downstream service.
- **503** - if the downstream request times out.

### 14.3 Design

Historically Ocelot errors are implemented by the [HttpExceptionToErrorMapper](#) class. The `Map` method converts a `System.Exception` object to native `Ocelot.Errors.Error` object.

We do HTTP status code overriding because of Exception-to-Error mapping. This can be confusing for the developer since the actual status code of the downstream service may be different and get lost. Please, research and review all response headers of upstream service. If you did not find statuses and (or) required headers then [Headers Transformation](#) feature should help.

We expect you to share your user case with us in the [Discussions](#) space of the repository. 





## GRAPHQL

Ocelot doesn't directly support [GraphQL](#), but so many people have asked about it. We wanted to show how easy it is to integrate the [GraphQL for .NET](#) library.

Please see the sample project [OcelotGraphQL](#). Using a combination of the [graphql-dotnet](#) project and Ocelot [Delegating Handlers](#) features, this is pretty easy to do. However we do not intend to integrate more closely with **GraphQL** at the moment. Check out the samples [README.md](#) and that should give you enough instruction on how to do this!

### 15.1 Future

If you have sufficient experience with GraphQL and mentioned [.NET package](#), we would welcome your contribution to the sample. 🐙

Who knows, maybe you'll get inspired by the sample development and come up with some design solution in the form of a rough draft of GraphQL feature to implement in Ocelot. Good luck!

And, welcome to [Discussions](#) space of the repository!





## HEADERS TRANSFORMATION

Ocelot allows the user to transform headers pre and post downstream request. At the moment Ocelot only supports find and replace. This feature was requested in [issue 190](#) and the team decided that it was going to be useful in various ways.

### 16.1 Add to Request

This feature was requested in [issue 313](#).

If you want to add a header to your upstream request please add the following to a Route in your **ocelot.json**:

```
"UpstreamHeaderTransform": {  
  "Uncle": "Bob"  
}
```

In the example above a header with the key **Uncle** and value **Bob** would be send to to the upstream service.

Placeholders are supported too (see below).

### 16.2 Add to Response

This feature was requested in [issue 280](#).

If you want to add a header to your downstream response, please add the following to a Route in **ocelot.json**:

```
"DownstreamHeaderTransform": {  
  "Uncle": "Bob"  
}
```

In the example above a header with the key **Uncle** and value **Bob** would be returned by Ocelot when requesting the specific Route.

If you want to return the [Butterfly APM](#) trace id then do something like the following:

```
"DownstreamHeaderTransform": {  
  "AnyKey": "{TraceId}"  
}
```

## 16.3 Find and Replace

In order to transform a header first we specify the header key and then the type of transform we want e.g.

```
"Test": "http://www.bbc.co.uk/, http://ocelot.com/"
```

The key is `Test` and the value is `http://www.bbc.co.uk/, http://ocelot.com/`. The value is saying: replace `http://www.bbc.co.uk/` with `http://ocelot.com/`. The syntax is `{find}, {replace}`. Hopefully pretty simple. There are examples below that explain more.

## 16.4 Pre Downstream Request

Add the following to a Route in `ocelot.json` in order to replace `http://www.bbc.co.uk/` with `http://ocelot.com/`. This header will be changed before the request downstream and will be sent to the downstream server.

```
"UpstreamHeaderTransform": {  
  "Test": "http://www.bbc.co.uk/, http://ocelot.com/"  
}
```

## 16.5 Post Downstream Request

Add the following to a Route in `ocelot.json` in order to replace `http://www.bbc.co.uk/` with `http://ocelot.com/`. This transformation will take place after Ocelot has received the response from the downstream service.

```
"DownstreamHeaderTransform": {  
  "Test": "http://www.bbc.co.uk/, http://ocelot.com/"  
}
```

## 16.6 Placeholders

Ocelot allows placeholders that can be used in header transformation.

- `{BaseUrl}` - This will use Ocelot base URL e.g. `http://localhost:5000` as its value.
- `{DownstreamBaseUrl}` - This will use the downstream services base URL e.g. `http://localhost:5000` as its value. This only works for **DownstreamHeaderTransform** at the moment.
- `{RemoteIpAddress}` - This will find the clients IP address using `IHttpContextAccessor.HttpContext.Connection.RemoteIpAddress.ToString()`, so you will get back some IP. See more in the [GetRemoteIpAddress](#) method.
- `{TraceId}` - This will use the [Butterfly APM](#) Trace Id. This only works for **DownstreamHeaderTransform** at the moment.
- `{UpstreamHost}` - This will look for the incoming Host header.

For now, we believe these placeholders are sufficient for basic user scenarios. But if you need more placeholders, you can head to the *future*.

## 16.7 Handling 302 Redirects

Ocelot will by default automatically follow redirects, however if you want to return the location header to the client, you might want to change the location to be Ocelot not the downstream service. Ocelot allows this with the following configuration:

```
"DownstreamHeaderTransform": {
  "Location": "http://www.bbc.co.uk/, http://ocelot.com/"
},
"HttpHandlerOptions": {
  "AllowAutoRedirect": false,
}
```

Or, you could use the **BaseUrl** placeholder.

```
"DownstreamHeaderTransform": {
  "Location": "http://localhost:6773, {BaseUrl}"
},
"HttpHandlerOptions": {
  "AllowAutoRedirect": false,
}
```

Finally, if you are using a load balancer with Ocelot, you will get multiple downstream base URLs so the above would not work. In this case you can do the following:

```
"DownstreamHeaderTransform": {
  "Location": "{DownstreamBaseUrl}, {BaseUrl}"
},
"HttpHandlerOptions": {
  "AllowAutoRedirect": false,
}
```

## 16.8 X-Forwarded-For

An example of using `{RemoteIpAddress}` placeholder:

```
"UpstreamHeaderTransform": {
  "X-Forwarded-For": "{RemoteIpAddress}"
}
```

## 16.9 Future

Ideally this feature would be able to support the fact that a header can have multiple values. At the moment it just assumes one. It would also be nice if it could multi find and replace e.g.

```
"DownstreamHeaderTransform": {
  "Location": "[{one,one},{two,two}]"
},
"HttpHandlerOptions": {
```

(continues on next page)


(continued from previous page)

```
"AllowAutoRedirect": false,  
}
```

If anyone wants to have a go at this please, help yourself!

### 16.9.1 Global Headers Transformation

We have pending open [PR 1659](#) for the [1658](#) issue. Current [20.0](#) version provides Route-level *Headers Transformation* feature, but we hope **global** transformations will be included in the next upcoming [release](#).

Any ideas and proposals can be shared in the [Discussions](#) space of the repository! 



## KUBERNETES

### Feature: *Service Discovery*

This feature was requested as part of [issue 345](#) to add support for [Kubernetes](#) service discovery provider.

Ocelot will call the K8s endpoints API in a given namespace to get all of the endpoints for a pod and then load balance across them. Ocelot used to use the services API to send requests to the K8s service but this was changed in [PR 1134](#) because the service did not load balance as expected.

The first thing you need to do is install the [NuGet package](#) that provides Kubernetes support in Ocelot:

```
Install-Package Ocelot.Provider.Kubernetes
```

Then add the following to your `ConfigureServices` method:

```
services.AddOcelot().AddKubernetes();
```

If you have services deployed in Kubernetes, you will normally use the naming service to access them. Default `usePodServiceAccount = true`, which means that Service Account using Pod to access the service of the K8s cluster needs to be Service Account based on RBAC authorization:

```
public static class OcelotBuilderExtensions
{
    public static IOcelotBuilder AddKubernetes(this IOcelotBuilder builder, bool_
↪ usePodServiceAccount = true);
}
```

You can replicate a `Permissive` using RBAC role bindings (see [Permissive RBAC Permissions](#)), K8s API server and token will read from pod.

```
kubectl create clusterrolebinding permissive-binding --clusterrole=cluster-admin --
↪ user=admin --user=kubelet --group=system:serviceaccounts
```

The following example shows how to set up a Route that will work in Kubernetes. The most important thing is the **ServiceName** which is made up of the Kubernetes service name. We also need to set up the **ServiceDiscoveryProvider** in **GlobalConfiguration**. The example here shows a typical configuration:

```
{
  "Routes": [
    {
      "DownstreamPathTemplate": "/api/values",
      "DownstreamScheme": "http",
      "UpstreamPathTemplate": "/values",
```

(continues on next page)

(continued from previous page)

```

    "ServiceName": "downstreamservice",
    "UpstreamHttpMethod": [ "Get" ]
  },
  ],
  "GlobalConfiguration": {
    "ServiceDiscoveryProvider": {
      "Host": "192.168.0.13",
      "Port": 443,
      "Token": "txpc696iUhbVoudg164r93CxDTTrKRVWG",
      "Namespace": "dev",
      "Type": "kube"
    }
  }
}

```

Service deployment in **Namespace** dev, **ServiceDiscoveryProvider** type is kube, you also can set pollkube **ServiceDiscoveryProvider** type. Note: **Host**, **Port** and **Token** are no longer in use.

You use Ocelot to poll Kubernetes for latest service information rather than per request. If you want to poll Kubernetes for the latest services rather than per request (default behaviour) then you need to set the following configuration:

```

"ServiceDiscoveryProvider": {
  // ...
  "Namespace": "dev",
  "Type": "pollkube",
  "PollingInterval": 100
}

```

The polling interval is in milliseconds and tells Ocelot how often to call Kubernetes for changes in service configuration.

Please note, there are tradeoffs here. If you poll Kubernetes, it is possible Ocelot will not know if a service is down depending on your polling interval and you might get more errors than if you get the latest services per request. This really depends on how volatile your services are. We doubt it will matter for most people and polling may give a tiny performance improvement over calling Kubernetes per request. There is no way for Ocelot to work these out for you.

If your downstream service resides in a different namespace, you can override the global setting at the Route-level by specifying a **ServiceNamespace**:

```

"Routes": [
  {
    // ...
    "ServiceName": "downstreamservice",
    "ServiceNamespace": "downstream-namespace"
  }
]

```

## LOAD BALANCER

Ocelot can load balance across available downstream services for each Route. This means you can scale your downstream services and Ocelot can use them effectively.

The types of load balancer available are:

- **LeastConnection** tracks which services are dealing with requests and sends new requests to service with least existing requests. The algorithm state is not distributed across a cluster of Ocelot's.
- **RoundRobin** loops through available services and sends requests. The algorithm state is not distributed across a cluster of Ocelot's.
- **NoLoadBalancer** takes the first available service from config or service discovery.
- **CookieStickySessions** uses a cookie to stick all requests to a specific server. More info below.

You must choose in your configuration which load balancer to use.

### 18.1 Configuration

The following shows how to set up multiple downstream services for a Route using **ocelot.json** and then select the LeastConnection load balancer. This is the simplest way to get load balancing set up.

```
{
  "UpstreamPathTemplate": "/posts/{postId}",
  "UpstreamHttpMethod": [ "Put", "Delete" ],
  "DownstreamPathTemplate": "/api/posts/{postId}",
  "DownstreamScheme": "https",
  "DownstreamHostAndPorts": [
    { "Host": "10.0.1.10", "Port": 5000 },
    { "Host": "10.0.1.11", "Port": 5000 }
  ],
  "LoadBalancerOptions": {
    "Type": "LeastConnection"
  }
}
```

## 18.2 Service Discovery

The following shows how to set up a Route using service discovery then select the `LeastConnection` load balancer.

```
{
  // ...
  "ServiceName": "product",
  "LoadBalancerOptions": {
    "Type": "LeastConnection"
  }
}
```

When this is set up Ocelot will lookup the downstream host and port from the service discover provider and load balance requests across any available services. If you add and remove services from the service discovery provider (Consul) then Ocelot should respect this and stop calling services that have been removed and start calling services that have been added.

## 18.3 CookieStickySessions Type

We have implemented a really basic sticky session type of load balancer. The scenario it is meant to support is you have a bunch of downstream servers that don't share session state, so if you get more than one request for one of these servers then it should go to the same box each time or the session state might be incorrect for the given user. This feature was requested in [issue 322](#) though what the user wants is more complicated than just sticky sessions. Anyway, we thought this would be a nice feature to have!

In order to set up `CookieStickySessions` load balancer you need to do something like the following:

```
{
  "UpstreamPathTemplate": "/posts/{postId}",
  "UpstreamHttpMethod": [ "Put", "Delete" ],
  "DownstreamPathTemplate": "/api/posts/{postId}",
  "DownstreamScheme": "https",
  "DownstreamHostAndPorts": [
    { "Host": "10.0.1.10", "Port": 5000 },
    { "Host": "10.0.1.11", "Port": 5000 }
  ],
  "LoadBalancerOptions": {
    "Type": "CookieStickySessions",
    "Key": "ASP.NET_SessionId",
    "Expiry": 1800000
  }
}
```

The `LoadBalancerOptions` are

- **Type** this needs to be `CookieStickySessions`
- **Key** this is the key of the cookie you wish to use for the sticky sessions
- **Expiry** this is how long in milliseconds you want to the session to be stuck for. Remember this refreshes on every request which is meant to mimick how sessions work usually.

If you have multiple Routes with the same `LoadBalancerOptions` then all of those Routes will use the same load balancer for there subsequent requests. This means the sessions will be stuck across Routes.



Please note that if you give more than one **DownstreamHostAndPort** or you are using a Service Discovery provider such as Consul and this returns more than one service then **CookieStickySessions** uses round robin to select the next server. This is hard coded at the moment but could be changed.

## 18.4 Custom Load Balancers

David Lievrouw implemented a way to provide Ocelot with custom load balancer in [PR 1155](#) (his [issue 961](#)).

In order to create and use a custom load balancer you can do the following. Below we setup a basic load balancing config and not the **Type** is CustomLoadBalancer which is the name of a class we will setup to do load balancing.

```
{
  "UpstreamPathTemplate": "/posts/{postId}",
  "UpstreamHttpMethod": [ "Put", "Delete" ],
  "DownstreamPathTemplate": "/api/posts/{postId}",
  "DownstreamScheme": "https",
  "DownstreamHostAndPorts": [
    { "Host": "10.0.1.10", "Port": 5000 },
    { "Host": "10.0.1.11", "Port": 5000 }
  ],
  "LoadBalancerOptions": {
    "Type": "CustomLoadBalancer"
  }
}
```

Then you need to create a class that implements the `ILoadBalancer` interface. Below is a simple round robin example:

```
public class CustomLoadBalancer : ILoadBalancer
{
    private readonly Func<Task<List<Service>>> _services;
    private readonly object _lock = new object();
    private int _last;

    public CustomLoadBalancer(Func<Task<List<Service>>> services)
    {
        _services = services;
    }

    public async Task<Response<ServiceHostAndPort>> Lease(HttpContext httpContext)
    {
        var services = await _services?.Invoke();
        lock (_lock)
        {
            if (_last >= services.Count)
                _last = 0;

            var next = services[_last++];
            return new OkResponse<ServiceHostAndPort>(next.HostAndPort);
        }
    }

    public void Release(ServiceHostAndPort hostAndPort) { }
}
```

Finally, you need to register this class with Ocelot.

We have used the most complex example below to show all of the data / types that can be passed into the factory that creates load balancers.

```
Func<IServiceProvider, DownstreamRoute, IServiceDiscoveryProvider, CustomLoadBalancer>␣  
↪loadBalancerFactoryFunc =  
    (serviceProvider, Route, serviceDiscoveryProvider) => new␣  
↪CustomLoadBalancer(serviceDiscoveryProvider.Get);  
  
services.AddOcelot()  
    .AddCustomLoadBalancer(loadBalancerFactoryFunc);
```

However, there is a much simpler example that will work the same:

```
services.AddOcelot()  
    .AddCustomLoadBalancer<CustomLoadBalancer>();
```

There are numerous extension methods to add a custom load balancer and the interface is as follows:

```
IOcelotBuilder AddCustomLoadBalancer<T>()  
    where T : ILoadBalancer, new();  
  
IOcelotBuilder AddCustomLoadBalancer<T>(Func<T> loadBalancerFactoryFunc)  
    where T : ILoadBalancer;  
  
IOcelotBuilder AddCustomLoadBalancer<T>(Func<IServiceProvider, T>␣  
↪loadBalancerFactoryFunc)  
    where T : ILoadBalancer;  
  
IOcelotBuilder AddCustomLoadBalancer<T>(Func<DownstreamRoute, IServiceDiscoveryProvider,␣  
↪T> loadBalancerFactoryFunc)  
    where T : ILoadBalancer;  
  
IOcelotBuilder AddCustomLoadBalancer<T>(Func<IServiceProvider, DownstreamRoute,␣  
↪IServiceDiscoveryProvider, T> loadBalancerFactoryFunc)  
    where T : ILoadBalancer;
```

When you enable custom load balancers Ocelot looks up your load balancer by its class name when it decides if it should do load balancing. If it finds a match, it will use your load balancer to load balance. If Ocelot cannot match the load balancer type in your configuration with the name of registered load balancer class then you will receive a [HTTP 500 Internal Server Error](#). If your load balancer factory throw an exception when Ocelot calls it, you will receive a [HTTP 500 Internal Server Error](#).

Remember, if you specify no load balancer in your config, Ocelot will not try and load balance.

## LOGGING

Ocelot uses the standard logging interfaces `ILoggerFactory` and `ILogger<T>` at the moment. This is encapsulated in `IOcelotLogger` and `IOcelotLoggerFactory` with an implementation for the standard [ASP.NET Core logging](#) stuff at the moment. This is because Ocelot adds some extra info to the logs such as **request ID** if it is configured.

There is a global [error handler middleware](#) that should catch any exceptions thrown and log them as errors.

Finally, if logging is set to **Trace** level, Ocelot will log starting, finishing and any middlewares that throw an exception which can be quite useful.

The reason for not just using [bog standard](#) framework logging is that we could not work out how to override the request id that get's logged when setting **IncludeScopes** to `true` for logging settings. Nicely onto the next feature.

### 19.1 Warning

If you are logging to [Console](#), you will get terrible performance. The team has had so many issues about performance issues with Ocelot and it is always logging level **Debug**, logging to [Console](#).

- **Warning!** Make sure you are logging to something proper in production environment!
- Use **Error** and **Critical** levels in production environment!
- Use **Warning** level in testing environment!



## METHOD TRANSFORMATION

Ocelot allows the user to change the HTTP request method that will be used when making a request to a downstream service.

This achieved by setting the following Route configuration:

```
{
  "UpstreamPathTemplate":("/{url}",
  "DownstreamPathTemplate":("/{url}",
  "DownstreamScheme": "http",
  "DownstreamHostAndPorts": [
    { "Host": "localhost", "Port": 54321 }
  ],
  "UpstreamHttpMethod": [ "Get" ],
  "DownstreamHttpMethod": "POST" // !
}
```

The key property here is **DownstreamHttpMethod** which is set as POST and the Route will only match on GET as set by **UpstreamHttpMethod**.

This feature can be useful when interacting with downstream APIs that only support POST and you want to present some kind of RESTful interface.



## MIDDLEWARE INJECTION

Warning, use with caution! If you are seeing any exceptions or strange behavior in your middleware pipeline and you are using any of the following. Remove them and try again!

When setting up Ocelot in your **Startup.cs** you can provide some additional middleware and override middleware. This is done as follows:

```
var configuration = new OcelotPipelineConfiguration
{
    PreErrorResponderMiddleware = async (context, next) =>
    {
        await next.Invoke();
    }
};
app.UseOcelot(configuration);
```

In the example above the provided function will run before the first piece of Ocelot middleware. This allows a user to supply any behaviors they want before and after the Ocelot pipeline has run. This means you can break everything, so use at your own pleasure!

The user can set functions against the following (see more in the [OcelotPipelineConfiguration](#) class):

- **PreErrorResponderMiddleware** injection is already explained above.
- **PreAuthenticationMiddleware** injection allows the user to run pre authentication logic and then call Ocelot authentication middleware.
- **AuthenticationMiddleware** overrides Ocelot authentication middleware.<sup>1</sup>
- **PreAuthorizationMiddleware** injection allows the user to run pre authorization logic and then call Ocelot authorization middleware.
- **AuthorizationMiddleware** overrides Ocelots authorization middleware.[Page 65, 1](#)
- **PreQueryStringBuilderMiddleware** injection allows the user to manipulate the query string on the http request before it is passed to Ocelot request creator.

Obviously you can just add mentioned Ocelot middleware overrides as normal before the call to `app.UseOcelot()`. It cannot be added after as Ocelot does not call the next Ocelot middleware overrides based on specified middleware configuration. So, the next called middlewares **will not** affect Ocelot configuration.

---

<sup>1</sup> **Warning, use mentioned middlewares overrides with caution!** Overridden middleware removes the default implementation! If you are seeing any exceptions or strange behavior in your middleware pipeline, remove overridden middlewares and try again!

## 21.1 ASP.NET Core Middlewares and Ocelot Pipeline Builder

Ocelot pipeline is a part of entire [ASP.NET Core Middlewares](#) conveyor aka app pipeline. The [BuildOcelotPipeline](#) method encapsulates Ocelot pipeline. The last middleware in the `BuildOcelotPipeline` method is `HttpRequesterMiddleware` that calls the next middleware, if added to the pipeline.

The internal [HttpRequesterMiddleware](#) is part of the pipeline but it is private and cannot be overridden, since this middleware does not belong to the list of user's public ones that can be overridden! So, this is the last middleware of the entire Ocelot and ASP.NET pipeline, and it handles non-user operation. The last user (public) middleware that can be overridden is [PreQueryStringBuilderMiddleware](#) being read from the pipeline configuration object, see *previous section*.

Considering that `PreQueryStringBuilderMiddleware` and `HttpRequesterMiddleware` are the last user and system middlewares, there are no other middlewares in the pipeline at all. But you can still extend the ASP.NET pipeline, as shown in the following code:


```
app.UseOcelot().Wait();
app.UseMiddleware<MyCustomMiddleware>();
```

But we do not recommend adding this custom middleware before or after calling of `UseOcelot()` as it affects the stability of the entire pipeline and has not been tested. Such kind of custom pipeline building is out of the Ocelot pipeline model and the quality of the solution is at your own risk.

Finally, do not get confused about the distinction between system (private, non-overridden) and user (public, overridden) middlewares. Private middlewares are hidden and cannot be overridden, but the entire ASP.NET pipeline can still be extended. The [public middlewares](#) are fully customizable and can be overridden.

## 21.2 Future

The community shows an interest in adding more overridden middlewares. One of such request is [PR 1497](#), and possibly it will be included in a next upcoming [release](#).

Anyway, in your opinion, if current overridden middlewares do not provide enough pipeline flexibility, you can open new topic in [Discussions](#) space of the repository. 

---



## QUALITY OF SERVICE

Label: QoS

Ocelot supports one QoS capability at the current time. You can set on a per Route basis if you want to use a circuit breaker when making requests to a downstream service. This uses an awesome .NET library called [Polly](#), check them out in [official repo](#).

The first thing you need to do if you want to use the *Administration* API is bring in the relevant NuGet [package](#):

```
Install-Package Ocelot.Provider.Polly
```

Then in your `ConfigureServices` method to add Polly services we must call the `AddPolly()` extension of the `OcelotBuilder` being returned by `AddOcelot()`<sup>1</sup> like below:

```
services.AddOcelot()  
    .AddPolly();
```

Then add the following section to a Route configuration:

```
"QoSOptions": {  
  "ExceptionsAllowedBeforeBreaking": 3,  
  "DurationOfBreak": 1000,  
  "TimeoutValue": 5000  
}
```

- You must set a number greater than 0 against **ExceptionsAllowedBeforeBreaking** for this rule to be implemented.<sup>2</sup>
- **DurationOfBreak** means the circuit breaker will stay open for 1 second after it is tripped.
- **TimeoutValue** means if a request takes more than 5 seconds, it will automatically be timed out.

You can set the **TimeoutValue** in isolation of the **ExceptionsAllowedBeforeBreaking** and **DurationOfBreak** options:

```
"QoSOptions": {  
  "TimeoutValue": 5000  
}
```

There is no point setting the other two in isolation as they affect each other!

If you do not add a QoS section, QoS will not be used, however Ocelot will default to a 90 seconds timeout on all downstream requests. If someone needs this to be configurable, open an issue.<sup>Page 67, 2</sup>

---

<sup>1</sup> The `AddOcelot` method adds default ASP.NET services to DI-container. You could call another more extended `AddOcelotUsingBuilder` method while configuring services to build and use custom builder via an `IMvcCoreBuilder` interface object. See more instructions in [Dependency Injection](#), “[The AddOcelotUsingBuilder method](#)” section.

<sup>2</sup> If something doesn't work or you get stuck, please review current [QoS issues](#) filtering by label.



## RATE LIMITING

### 23.1 Ocelot Own Implementation

Ocelot supports rate limiting of upstream requests so that your downstream services do not become overloaded.

The authors of this feature were inspired by [@catcherwong](#) article to finally write this documentation. This feature was added by [@geffzhang](#) on GitHub! Thanks very much!

To get rate limiting working for a Route you need to add the following JSON to it:

```
"RateLimitOptions": {  
  "ClientWhitelist": [],  
  "EnableRateLimiting": true,  
  "Period": "1s",  
  "PeriodTimespan": 1,  
  "Limit": 1  
}
```

- **ClientWhitelist** - This is an array that contains the whitelist of the client. It means that the client in this array will not be affected by the rate limiting.
- **EnableRateLimiting** - This value specifies enable endpoint rate limiting.
- **Period** - This value specifies the period that the limit applies to, such as 1s, 5m, 1h, 1d and so on. If you make more requests in the period than the limit allows then you need to wait for **PeriodTimespan** to elapse before you make another request.
- **PeriodTimespan** - This value specifies that we can retry after a certain number of seconds.
- **Limit** - This value specifies the maximum number of requests that a client can make in a defined period.

You can also set the following in the **GlobalConfiguration** part of **ocelot.json**:

```
"GlobalConfiguration": {  
  "BaseUrl": "https://api.mybusiness.com",  
  "RateLimitOptions": {  
    "DisableRateLimitHeaders": false,  
    "QuotaExceededMessage": "Customize Tips!",  
    "HttpStatusCode": 123,  
    "ClientIdHeader": "Test"  
  }  
}
```

- **DisableRateLimitHeaders** - This value specifies whether X-Rate-Limit and Retry-After headers are disabled.

- **QuotaExceededMessage** - This value specifies the exceeded message.
- **HttpStatusCode** - This value specifies the returned HTTP status code when rate limiting occurs.
- **ClientIdHeader** - Allows you to specify the header that should be used to identify clients. By default it is `ClientId`

## 23.2 Future and ASP.NET Core Implementation

The Ocelot team considers to redesign *Rate Limiting* feature, because of [Announcing Rate Limiting for .NET](#) by Brennan Conroy on July 13th, 2022. There is no decision at the moment, and the old version of the feature is included as a part of release 20.0 for .NET 7.

See more about new feature being added into ASP.NET Core 7.0 release:

- [RateLimiter Class](#), since ASP.NET Core 7.0
- [System.Threading.RateLimiting](#) NuGet package
- [Rate limiting middleware in ASP.NET Core](#) article by Arvin Kahbazi, Maarten Balliauw, and Rick Anderson

However, it makes sense to keep the old implementation as a Ocelot built-in native feature, but we are going to migrate to the new Rate Limiter from `Microsoft.AspNetCore.RateLimiting` namespace.

Please, share your opinion to us in the [Discussions](#) space of the repository.



## REQUEST AGGREGATION

Ocelot allows you to specify Aggregate Routes that compose multiple normal Routes and map their responses into one object. This is usually where you have a client that is making multiple requests to a server where it could just be one. This feature allows you to start implementing back-end for a front-end (BFF) type architecture with Ocelot.

This feature was requested as part of [issue 79](#) and further improvements were made as part of [issue 298](#).

In order to set this up you must do something like the following in your **ocelot.json**. Here we have specified two normal Routes and each one has a **Key** property. We then specify an Aggregate that composes the two Routes using their keys in the **RouteKeys** list and says then we have the **UpstreamPathTemplate** which works like a normal Route. Obviously you cannot have duplicate **UpstreamPathTemplates** between **Routes** and **Aggregates**. You can use all of Ocelot's normal Route options apart from **RequestIdKey** (explained in *gotchas* below).

### 24.1 Advanced Register Your Own Aggregators

Ocelot started with just the basic request aggregation and since then we have added a more advanced method that let's the user take in the responses from the downstream services and then aggregate them into a response object.

The **ocelot.json** setup is pretty much the same as the basic aggregation approach apart from you need to add an **Aggregator** property like below:

```
{
  "Routes": [
    {
      "UpstreamHttpMethod": [ "Get" ],
      "UpstreamPathTemplate": "/laura",
      "DownstreamPathTemplate": "/",
      "DownstreamScheme": "http",
      "DownstreamHostAndPorts": [
        { "Host": "localhost", "Port": 51881 }
      ],
      "Key": "Laura" // <--
    },
    {
      "UpstreamHttpMethod": [ "Get" ],
      "UpstreamPathTemplate": "/tom",
      "DownstreamPathTemplate": "/",
      "DownstreamScheme": "http",
      "DownstreamHostAndPorts": [
        { "Host": "localhost", "Port": 51882 }
      ],
    },
  ],
}
```

(continues on next page)

(continued from previous page)

```

        "Key": "Tom" // <--
    },
    "Aggregates": [
        {
            "UpstreamPathTemplate": "/",
            "RouteKeys": [
                "Tom",
                "Laura"
            ],
            "Aggregator": "FakeDefinedAggregator"
        }
    ]
}

```

Here we have added an aggregator called `FakeDefinedAggregator`. Ocelot is going to look for this aggregator when it tries to aggregate this Route.

In order to make the aggregator available we must add the `FakeDefinedAggregator` to the `OcelotBuilder` being returned by `AddOcelot()`<sup>1</sup> like below:

```

services
    .AddOcelot()
    .AddSingletonDefinedAggregator<FakeDefinedAggregator>();

```

Now when Ocelot tries to aggregate the Route above it will find the `FakeDefinedAggregator` in the container and use it to aggregate the Route. Because the `FakeDefinedAggregator` is registered in the container you can add any dependencies it needs into the container like below:

```

services.AddSingleton<FooDependency>();
// ...
services.AddOcelot()
    .AddSingletonDefinedAggregator<FooAggregator>();

```

In this example `FooAggregator` takes a dependency on `FooDependency` and it will be resolved by the container.

In addition to this Ocelot lets you add transient aggregators like below:

```

services
    .AddOcelot()
    .AddTransientDefinedAggregator<FakeDefinedAggregator>();

```

In order to make an Aggregator you must implement this interface:

```

public interface IDefinedAggregator
{
    Task<DownstreamResponse> Aggregate(List<HttpContext> responses);
}

```

With this feature you can pretty much do whatever you want because the `HttpContext` objects contain the results of all the aggregate requests. Please note, if the `HttpClient` throws an exception when making a request to a Route in the

<sup>1</sup> The `AddOcelot` method adds default ASP.NET services to DI-container. You could call another more extended `AddOcelotUsingBuilder` method while configuring services to build and use custom builder via an `IMvcCoreBuilder` interface object. See more instructions in [Dependency Injection](#), “The `AddOcelotUsingBuilder` method” section.

aggregate then you will not get a `HttpContext` for it, but you would for any that succeed. If it does throw an exception, this will be logged.

## 24.2 Basic Expecting JSON from Downstream Services

```
{
  "Routes": [
    {
      "UpstreamHttpMethod": [ "Get" ],
      "UpstreamPathTemplate": "/laura",
      "DownstreamPathTemplate": "/",
      "DownstreamScheme": "http",
      "DownstreamHostAndPorts": [
        { "Host": "localhost", "Port": 51881 }
      ],
      "Key": "Laura"
    },
    {
      "UpstreamHttpMethod": [ "Get" ],
      "UpstreamPathTemplate": "/tom",
      "DownstreamPathTemplate": "/",
      "DownstreamScheme": "http",
      "DownstreamHostAndPorts": [
        { "Host": "localhost", "Port": 51882 }
      ],
      "Key": "Tom"
    }
  ],
  "Aggregates": [
    {
      "UpstreamPathTemplate": "/",
      "RouteKeys": [
        "Tom",
        "Laura"
      ]
    }
  ]
}
```

You can also set **UpstreamHost** and **RouteIsCaseSensitive** in the Aggregate configuration. These behave the same as any other Routes.

If the Route `/tom` returned a body of `{"Age": 19}` and `/laura` returned `{"Age": 25}`, the the response after aggregation would be as follows:

```
{"Tom":{"Age": 19},"Laura":{"Age": 25}}
```

At the moment the aggregation is very simple. Ocelot just gets the response from your downstream service and sticks it into a JSON dictionary as above. With the Route key being the key of the dictionary and the value the response body from your downstream service. You can see that the object is just JSON without any pretty spaces etc.

Note, all headers will be lost from the downstream services response.

Ocelot will always return content type `application/json` with an aggregate request.

If you downstream services return a [404 Not Found](#), the aggregate will just return nothing for that downstream service. It will not change the aggregate response into a **404** even if all the downstreams return a **404**.

## 24.3 Gotchas

You cannot use Routes with specific **RequestIdKeys** as this would be crazy complicated to track.

Aggregation only supports the GET HTTP verb.

---



## REQUEST ID

### aka **Correlation ID**

Ocelot supports a client sending a *request ID* in the form of a header. If set, Ocelot will use the **requestId** for logging as soon as it becomes available in the middleware pipeline. Ocelot will also forward the *request ID* with the specified header to the downstream service.

You can still get the ASP.NET Core *request ID* in the logs if you set **IncludeScopes** true in your logging config.

In order to use the *Request ID* feature you have two options.

### 25.1 Global

In your **ocelot.json** set the following in the **GlobalConfiguration** section. This will be used for all requests into Ocelot.

```
"GlobalConfiguration": {  
  "RequestIdKey": "OcRequestId"  
}
```

We recommend using the **GlobalConfiguration** unless you really need it to be Route specific.

### 25.2 Route

If you want to override this for a specific Route, add the following to **ocelot.json** for the specific Route:

```
"RequestIdKey": "OcRequestId"
```

Once Ocelot has identified the incoming requests matching Route object it will set the *request ID* based on the Route configuration.

### 25.3 Gotcha

This can lead to a small gotcha. If you set a **GlobalConfiguration**, it is possible to get one *request ID* until the Route is identified and then another after that because the *request ID* key can change. This is by design and is the best solution we can think of at the moment. In this case the **OcelotLogger** will show the *request ID* and previous *request ID* in the logs.

Below is an example of the logging when set at Debug level for a normal request:

```
dbug: Ocelot.Errors.Middleware.ExceptionHandlerMiddleware[0]
      requestId: asdf, previousRequestId: no previous request id, message: ocelot_
↳ pipeline started,
dbug: Ocelot.DownstreamRouteFinder.Middleware.DownstreamRouteFinderMiddleware[0]
      requestId: asdf, previousRequestId: no previous request id, message: upstream url_
↳ path is {upstreamUrlPath},
dbug: Ocelot.DownstreamRouteFinder.Middleware.DownstreamRouteFinderMiddleware[0]
      requestId: asdf, previousRequestId: no previous request id, message: downstream_
↳ template is {downstreamRoute.Data.Route.DownstreamPath},
dbug: Ocelot.RateLimit.Middleware.ClientRateLimitMiddleware[0]
      requestId: asdf, previousRequestId: no previous request id, message:_
↳ EndpointRateLimiting is not enabled for Ocelot.Values.PathTemplate,
dbug: Ocelot.Authorization.Middleware.AuthorizationMiddleware[0]
      requestId: 1234, previousRequestId: asdf, message: /posts/{postId} route does not_
↳ require user to be authorized,
dbug: Ocelot.DownstreamUrlCreator.Middleware.DownstreamUrlCreatorMiddleware[0]
      requestId: 1234, previousRequestId: asdf, message: downstream url is
↳ {downstreamUrl.Data.Value},
dbug: Ocelot.Request.Middleware.HttpRequestBuilderMiddleware[0]
      requestId: 1234, previousRequestId: asdf, message: setting upstream request,
dbug: Ocelot.Requester.Middleware.HttpRequesterMiddleware[0]
      requestId: 1234, previousRequestId: asdf, message: setting http response message,
dbug: Ocelot.Responder.Middleware.ResponderMiddleware[0]
      requestId: 1234, previousRequestId: asdf, message: no pipeline errors, setting and_
↳ returning completed response,
dbug: Ocelot.Errors.Middleware.ExceptionHandlerMiddleware[0]
      requestId: 1234, previousRequestId: asdf, message: ocelot pipeline finished,
```

## ROUTING

Ocelot's primary functionality is to take incoming HTTP requests and forward them on to a downstream service. Ocelot currently only supports this in the form of another HTTP request (in the future this could be any transport mechanism).

Ocelot describes the routing of one request to another as a Route. In order to get anything working in Ocelot you need to set up a Route in the configuration.

```
{  
  "Routes": []  
}
```

To configure a Route you need to add one to the Routes JSON array.

```
{  
  "UpstreamHttpMethod": [ "Put", "Delete" ],  
  "UpstreamPathTemplate": "/posts/{postId}",  
  "DownstreamPathTemplate": "/api/posts/{postId}",  
  "DownstreamScheme": "https",  
  "DownstreamHostAndPorts": [  
    { "Host": "localhost", "Port": 80 }  
  ]  
}
```

The **DownstreamPathTemplate**, **DownstreamScheme** and **DownstreamHostAndPorts** define the URL that a request will be forwarded to.

The **DownstreamHostAndPorts** property is a collection that defines the host and port of any downstream services that you wish to forward requests to. Usually this will just contain a single entry, but sometimes you might want to load balance requests to your downstream services and Ocelot allows you add more than one entry and then select a load balancer.

The **UpstreamPathTemplate** property is the URL that Ocelot will use to identify which **DownstreamPathTemplate** to use for a given request. The **UpstreamHttpMethod** is used so Ocelot can distinguish between requests with different HTTP verbs to the same URL. You can set a specific list of HTTP methods or set an empty list to allow any of them.

## 26.1 Placeholders

In Ocelot you can add placeholders for variables to your Templates in the form of `{something}`. The placeholder variable needs to be present in both the **DownstreamPathTemplate** and **UpstreamPathTemplate** properties. When it is Ocelot will attempt to substitute the value in the **UpstreamPathTemplate** placeholder into the **DownstreamPathTemplate** for each request Ocelot processes.

You can also do a *Catch All* type of Route e.g.

```
{
  "UpstreamHttpMethod": [ "Get", "Post" ],
  "UpstreamPathTemplate":("/{everything}",
  "DownstreamPathTemplate": "/api/{everything}",
  "DownstreamScheme": "https",
  "DownstreamHostAndPorts": [
    { "Host": "localhost", "Port": 80 }
  ]
}
```

This will forward any path + query string combinations to the downstream service after the path `/api`.

**Note**, the default Routing configuration is case insensitive!

In order to change this you can specify on a per Route basis the following setting:

```
"RouteIsCaseSensitive": true
```

This means that when Ocelot tries to match the incoming upstream URL with an upstream template the evaluation will be case sensitive.

## 26.2 Catch All

Ocelot's routing also supports a *Catch All* style routing where the user can specify that they want to match all traffic.

If you set up your config like below, all requests will be proxied straight through. The placeholder `{url}` name is not significant, any name will work.

```
{
  "UpstreamHttpMethod": [ "Get" ],
  "UpstreamPathTemplate":("/{url}",
  "DownstreamPathTemplate": "/{url}",
  "DownstreamScheme": "https",
  "DownstreamHostAndPorts": [
    { "Host": "localhost", "Port": 80 }
  ]
}
```

The *Catch All* has a lower priority than any other Route. If you also have the Route below in your config then Ocelot would match it before the *Catch All*.

```
{
  "UpstreamHttpMethod": [ "Get" ],
  "UpstreamPathTemplate": "/",
  "DownstreamPathTemplate": "/",
```

(continues on next page)

(continued from previous page)

```
"DownstreamScheme": "https",
"DownstreamHostAndPorts": [
  { "Host": "10.0.10.1", "Port": 80 }
]
```

## 26.3 Upstream Host

This feature allows you to have Routes based on the *upstream host*. This works by looking at the Host header the client has used and then using this as part of the information we use to identify a Route.

In order to use this feature please add the following to your config:

```
{
  "UpstreamHost": "somedomain.com"
}
```

The Route above will only be matched when the Host header value is `somedomain.com`.

If you do not set **UpstreamHost** on a Route then any Host header will match it. This means that if you have two Routes that are the same, apart from the **UpstreamHost**, where one is null and the other set Ocelot will favour the one that has been set.

This feature was requested as part of [issue 216](#).

## 26.4 Priority

You can define the order you want your Routes to match the Upstream HttpRequest by including a **Priority** property in `ocelot.json`. See [issue 270](#) for reference.

```
{
  "Priority": 0
}
```

0 is the lowest priority, Ocelot will always use 0 for `/catchAll` Routes and this is still hardcoded. After that you are free to set any priority you wish.

e.g. you could have

```
{
  "UpstreamPathTemplate": "/goods/{catchAll}",
  "Priority": 0
}
```

and

```
{
  "UpstreamPathTemplate": "/goods/delete",
  "Priority": 1
}
```

In the example above if you make a request into Ocelot on `/goods/delete`, Ocelot will match `/goods/delete` Route. Previously it would have matched `/goods/{catchAll}`, because this is the first Route in the list!

## 26.5 Dynamic Routing

This feature was requested in [issue 340](#).

The idea is to enable dynamic routing when using a service discovery provider so you don't have to provide the Route config. See the docs [Service Discovery](#) if this sounds interesting to you.

## 26.6 Query Strings

Ocelot allows you to specify a query string as part of the **DownstreamPathTemplate** like the example below:

```
{
  "UpstreamHttpMethod": [ "Get" ],
  "UpstreamPathTemplate": "/api/units/{subscriptionId}/{unitId}/updates",
  "DownstreamPathTemplate": "/api/subscriptions/{subscriptionId}/updates?unitId={unitId}",
  "DownstreamScheme": "http",
  "DownstreamHostAndPorts": [
    { "Host": "localhost", "Port": 50110 }
  ]
}
```

In this example Ocelot will use the value from the `{unitId}` placeholder in the upstream path template and add it to the downstream request as a query string parameter called `unitId`!

Ocelot will also allow you to put query string parameters in the **UpstreamPathTemplate** so you can match certain queries to certain services:

```
{
  "UpstreamHttpMethod": [ "Get" ],
  "UpstreamPathTemplate": "/api/subscriptions/{subscriptionId}/updates?unitId={unitId}",
  "DownstreamPathTemplate": "/api/units/{subscriptionId}/{unitId}/updates",
  "DownstreamScheme": "http",
  "DownstreamHostAndPorts": [
    { "Host": "localhost", "Port": 50110 }
  ]
}
```

In this example Ocelot will only match requests that have a matching URL path and the query string starts with `unitId=something`. You can have other queries after this but you must start with the matching parameter. Also Ocelot will swap the `{unitId}` parameter from the query string and use it in the downstream request path.

## 26.7 Security Options

Ocelot allows you to manage multiple patterns for allowed/blocked IPs using the [IPAddressRange](#) package with [MPL-2.0 License](#).

This feature is designed to allow greater IP management in order to include or exclude a wide IP range via CIDR notation or IP range. The current patterns managed are the following:

- Single IP: 192.168.1.1
- IP Range: 192.168.1.1-192.168.1.250
- IP Short Range: 192.168.1.1-250
- IP Range with subnet: 192.168.1.0/255.255.255.0
- CIDR: 192.168.1.0/24
- CIDR for IPv6: fe80::/10
- The allowed/blocked lists are evaluated during configuration loading
- The **ExcludeAllowedFromBlocked** property is intended to provide the ability to specify a wide range of blocked IP addresses and allow a subrange of IP addresses. Default value: `false`
- The absence of a property in **SecurityOptions** is allowed, it takes the default value.

```
{
  "SecurityOptions": {
    "IPBlockedList": [ "192.168.0.0/23" ],
    "IPAllowedList": ["192.168.0.15", "192.168.1.15"],
    "ExcludeAllowedFromBlocked": true
  }
}
```

This feature was requested as part of [issue 1400](#).





## SERVICE DISCOVERY

Ocelot allows you to specify a *service discovery* provider and will use this to find the host and port for the downstream service to which Ocelot forwards the request. At the moment this is only supported in the **GlobalConfiguration** section, which means the same *service discovery* provider will be used for all Routes for which you specify a *ServiceName* at Route level.

### 27.1 Consul

**Namespace:** `Ocelot.Provider.Consul`

The first thing you need to do is install the `Ocelot.Provider.Consul` package that provides `Consul` support in Ocelot:

```
Install-Package Ocelot.Provider.Consul
```

Then add the following to your `ConfigureServices` method:

```
services.AddOcelot()  
    .AddConsul();
```

Currently there are 2 types of Consul *service discovery* providers: `Consul` and `PollConsul`. The default provider is `Consul`, which means that if `ConsulProviderFactory` cannot read, understand, or parse the **Type** property of the `ServiceProviderConfiguration` object, then a `Consul` provider instance is created by the factory.

Explore these types of providers and understand the differences in the subsections below.

#### 27.1.1 Consul Provider Type

**Class:** `Ocelot.Provider.Consul.Consul`

The following is required in the `GlobalConfiguration`. The **ServiceDiscoveryProvider** property is required, and if you do not specify a host and port, the Consul default ones will be used.

Please note the **Scheme** option defaults to HTTP. It was added in [PR 1154](#). It defaults to HTTP to not introduce a breaking change.

```
"ServiceDiscoveryProvider": {  
  "Scheme": "https",  
  "Host": "localhost",  
  "Port": 8500,  
  "Type": "Consul"  
}
```

In the future we can add a feature that allows Route specific configuration.

In order to tell Ocelot a Route is to use the *service discovery* provider for its host and port you must add the **ServiceName** and load balancer you wish to use when making requests downstream. At the moment Ocelot has a [RoundRobin](#) and [LeastConnection](#) algorithms you can use. If no load balancer is specified, Ocelot will not load balance requests.

```
{
  "ServiceName": "product",
  "LoadBalancerOptions": {
    "Type": "LeastConnection"
  }
}
```

When this is set up Ocelot will lookup the downstream host and port from the *service discovery* provider and load balance requests across any available services.

### 27.1.2 PollConsul Provider Type

**Class:** `Ocelot.Provider.Consul.PollConsul`

A lot of people have asked the team to implement a feature where Ocelot *polls Consul* for latest service information rather than per request. If you want to *poll Consul* for the latest services rather than per request (default behaviour) then you need to set the following configuration:

```
"ServiceDiscoveryProvider": {
  "Host": "localhost",
  "Port": 8500,
  "Type": "PollConsul",
  "PollingInterval": 100
}
```

The polling interval is in milliseconds and tells Ocelot how often to call Consul for changes in service configuration.

Please note, there are tradeoffs here. If you *poll Consul* it is possible Ocelot will not know if a service is down depending on your polling interval and you might get more errors than if you get the latest services per request. This really depends on how volatile your services are. We doubt it will matter for most people and polling may give a tiny performance improvement over calling Consul per request (as sidecar agent). If you are calling a remote Consul agent then polling will be a good performance improvement.

### 27.1.3 Service Definition

Your services need to be added to Consul something like below (C# style but hopefully this make sense)... The only important thing to note is not to add `http` or `https` to the `Address` field. We have been contacted before about not accepting scheme in `Address`. After reading [this](#) we do not think the scheme should be in there.

In C#

```
new AgentService()
{
    Service = "some-service-name",
    Address = "localhost",
    Port = 8080,
    ID = "some-id",
}
```

Or, in JSON

```
"Service": {
  "ID": "some-id",
  "Service": "some-service-name",
  "Address": "localhost",
  "Port": 8080
}
```

### 27.1.4 ACL Token

If you are using [ACL](#) with Consul, Ocelot supports adding the X-Consul-Token header. In order so this to work you must add the additional property below:

```
"ServiceDiscoveryProvider": {
  "Host": "localhost",
  "Port": 8500,
  "Type": "Consul",
  "Token": "footoken"
}
```

Ocelot will add this token to the Consul client that it uses to make requests and that is then used for every request.

## 27.2 Eureka

This feature was requested as part of [issue 262](#) to add support for [Netflix Eureka](#) service discovery provider. The main reason for this is it is a key part of [Steeltoe](#) which is something to do with [Pivotal!](#) Anyway enough of the background.

The first thing you need to do is install the [Ocelot.Provider.Eureka](#) package that provides Eureka support in Ocelot:

```
Install-Package Ocelot.Provider.Eureka
```

Then add the following to your `ConfigureServices` method.

```
s.AddOcelot().AddEureka();
```

Then in order to get this working add the following to `ocelot.json`:

```
"ServiceDiscoveryProvider": {
  "Type": "Eureka"
}
```

And following the guide [here](#) you may also need to add some stuff to `appsettings.json`. For example the JSON below tells the Steeltoe / Pivotal services where to look for the service discovery server and if the service should register with it:

```
"eureka": {
  "client": {
    "serviceUrl": "http://localhost:8761/eureka/",
    "shouldRegisterWithEureka": false,
    "shouldFetchRegistry": true
  }
}
```

(continues on next page)

(continued from previous page)

```
}
}
```

If **shouldRegisterWithEureka** is false then **shouldFetchRegistry** will default to `true`, so you need not it explicitly but left it in there.

Ocelot will now register all the necessary services when it starts up and if you have the JSON above will register itself with Eureka. One of the services polls Eureka every 30 seconds (default) and gets the latest service state and persists this in memory. When Ocelot asks for a given service it is retrieved from memory so performance is not a big problem.

Ocelot will use the scheme (`http`, `https`) set in Eureka if these values are not provided in **ocelot.json**

## 27.3 Dynamic Routing

This feature was requested in [issue 340](#). The idea is to enable dynamic routing when using a service discovery provider (see that section of the docs for more info). In this mode Ocelot will use the first segment of the upstream path to lookup the downstream service with the service discovery provider.

An example of this would be calling Ocelot with a URL like `https://api.mywebsite.com/product/products`. Ocelot will take the first segment of the path which is `product` and use it as a key to look up the service in Consul. If Consul returns a service, Ocelot will request it on whatever host and port comes back from Consul plus the remaining path segments in this case `products` thus making the downstream call `http://hostfromconsul:portfromconsul/products`. Ocelot will append any query string to the downstream URL as normal.

**Note**, in order to enable dynamic routing you need to have 0 Routes in your config. At the moment you cannot mix dynamic and configuration Routes. In addition to this you need to specify the Service Discovery provider details as outlined above and the downstream `http/https` scheme as **DownstreamScheme**.

In addition to that you can set **RateLimitOptions**, **QoSOptions**, **LoadBalancerOptions** and **HttpHandlerOptions**, **DownstreamScheme** (You might want to call Ocelot on `https` but talk to private services over `http`) that will be applied to all of the dynamic Routes.

The config might look something like:

```
{
  "Routes": [],
  "Aggregates": [],
  "GlobalConfiguration": {
    "RequestIdKey": null,
    "ServiceDiscoveryProvider": {
      "Host": "localhost",
      "Port": 8500,
      "Type": "Consul",
      "Token": null,
      "ConfigurationKey": null
    },
    "RateLimitOptions": {
      "ClientIdHeader": "ClientId",
      "QuotaExceededMessage": null,
      "RateLimitCounterPrefix": "ocelot",
      "DisableRateLimitHeaders": false,
      "HttpStatusCode": 429
    }
  },
}
```

(continues on next page)

(continued from previous page)

```

    "QoSOptions": {
      "ExceptionsAllowedBeforeBreaking": 0,
      "DurationOfBreak": 0,
      "TimeoutValue": 0
    },
    "BaseUrl": null,
    "LoadBalancerOptions": {
      "Type": "LeastConnection",
      "Key": null,
      "Expiry": 0
    },
    "DownstreamScheme": "http",
    "HttpHandlerOptions": {
      "AllowAutoRedirect": false,
      "UseCookieContainer": false,
      "UseTracing": false
    }
  }
}

```

Ocelot also allows you to set **DynamicRoutes** collection which lets you set rate limiting rules per downstream service. This is useful if you have for example a product and search service and you want to rate limit one more than the other. An example of this would be as follows:

```

{
  "DynamicRoutes": [
    {
      "ServiceName": "product",
      "RateLimitRule": {
        "ClientWhitelist": [],
        "EnableRateLimiting": true,
        "Period": "1s",
        "PeriodTimespan": 1000.0,
        "Limit": 3
      }
    }
  ],
  "GlobalConfiguration": {
    "RequestIdKey": null,
    "ServiceDiscoveryProvider": {
      "Host": "localhost",
      "Port": 8523,
      "Type": "Consul"
    },
    "RateLimitOptions": {
      "ClientIdHeader": "ClientId",
      "QuotaExceededMessage": "",
      "RateLimitCounterPrefix": "",
      "DisableRateLimitHeaders": false,
      "HttpStatusCode": 428
    },
    "DownstreamScheme": "http"
  }
}

```

(continues on next page)

(continued from previous page)

```
}
}
```

This configuration means that if you have a request come into Ocelot on `/product/*` then dynamic routing will kick in and Ocelot will use the rate limiting set against the product service in the **DynamicRoutes** section.

Please take a look through all of the docs to understand these options.

## 27.4 Custom Providers

Ocelot also allows you to create your own *Service Discovery* implementation. This is done by implementing the `IServiceDiscoveryProvider` interface, as shown in the following example:

```
public class MyServiceDiscoveryProvider : IServiceDiscoveryProvider
{
    private readonly DownstreamRoute _downstreamRoute;

    public MyServiceDiscoveryProvider(DownstreamRoute downstreamRoute)
    {
        _downstreamRoute = downstreamRoute;
    }

    public async Task<List<Service>> Get()
    {
        var services = new List<Service>();
        //...
        //Add service(s) to the list matching the _downstreamRoute
        return services;
    }
}
```

And set its class name as the provider type in `ocelot.json`:

```
"GlobalConfiguration": {
  "ServiceDiscoveryProvider": {
    "Type": "MyServiceDiscoveryProvider"
  }
}
```

Finally, in the application's `ConfigureServices` method, register a `ServiceDiscoveryFinderDelegate` to initialize and return the provider:

```
ServiceDiscoveryFinderDelegate serviceDiscoveryFinder = (provider, config, route) =>
{
    return new MyServiceDiscoveryProvider(route);
};
services.AddSingleton(serviceDiscoveryFinder);
services.AddOcelot();
```

## 27.4.1 Custom Provider Sample

In order to introduce a basic template for a custom Service Discovery provider, we've prepared a good sample:

**Link:** [samples / OcelotServiceDiscovery](#)

**Solution:** `Ocelot.Samples.ServiceDiscovery.sln`

This solution contains the following projects:

- *ApiGateway*
- *DownstreamService*

This solution is ready for any deployment. All services are bound, meaning all ports and hosts are prepared for immediate use (running in Visual Studio).

All instructions for running this solution are in [README.md](#).

### DownstreamService

This project provides a single downstream service that can be reused across *ApiGateway* routes. It has multiple **launch-Settings.json** profiles for your favorite launch and hosting scenarios: Visual Studio running sessions, Kestrel console hosting, and Docker deployments.

### ApiGateway

This project includes a custom *Service Discovery* provider and it only has route(s) to *DownstreamService* services in the **ocelot.json** file. You can add more routes!

The main source code for the custom provider is in the [ServiceDiscovery](#) folder: the `MyServiceDiscoveryProvider` and `MyServiceDiscoveryProviderFactory` classes. You are welcome to design and develop them!

Additionally, the cornerstone of this custom provider is the `ConfigureServices` method, where you can choose design and implementation options: simple or more complex:

```
builder.ConfigureServices(s =>
{
    // Perform initialization from application configuration or hardcode/choose the best
    ↪option.
    bool easyWay = true;

    if (easyWay)
    {
        // Design #1. Define a custom finder delegate to instantiate a custom provider
        ↪under the default factory, which is ServiceDiscoveryProviderFactory
        s.AddSingleton<ServiceDiscoveryFinderDelegate>((serviceProvider, config,
        ↪downstreamRoute)
            => new MyServiceDiscoveryProvider(serviceProvider, config, downstreamRoute));
    }
    else
    {
        // Design #2. Abstract from the default factory
        ↪(ServiceDiscoveryProviderFactory) and from FinderDelegate,
        // and create your own factory by implementing the
        ↪IServiceDiscoveryProviderFactory interface.
        s.RemoveAll<IServiceDiscoveryProviderFactory>();
    }
});
```

(continues on next page)

(continued from previous page)

```
s.AddSingleton<IServiceDiscoveryProviderFactory,
↳MyServiceDiscoveryProviderFactory>();

    // It will not be called, but it is necessary for internal validators, it is
↳also a lifehack
    s.AddSingleton<ServiceDiscoveryFinderDelegate>((serviceProvider, config,
↳downstreamRoute) => null);
    }

    s.AddOcelot();
});
```

The easy way, lite design means that you only design the provider class, and specify `ServiceDiscoveryFinderDelegate` object for default `ServiceDiscoveryProviderFactory` in Ocelot core.

A more complex design means that you design both provider and provider factory classes. After this, you need to add the `IServiceDiscoveryProviderFactory` interface to the DI container, removing the default registered `ServiceDiscoveryProviderFactory` class. Note that in this case the Ocelot pipeline will not use `ServiceDiscoveryProviderFactory` by default. Additionally, you do not need to specify "Type": "MyServiceDiscoveryProvider" in the **ServiceDiscoveryProvider** properties of the **GlobalConfiguration** settings. But you can leave this Type option for compatibility between both designs.



## SERVICE FABRIC

If you have services deployed in [Azure Service Fabric](#) you will normally use the naming service to access them.

The following example shows how to set up a Route that will work in *Service Fabric*. The most important thing is the **ServiceName** which is made up of the *Service Fabric* application name then the specific service name. We also need to set up the **ServiceDiscoveryProvider** in **GlobalConfiguration**. The example here shows a typical configuration. It assumes *Service Fabric* is running on localhost and that the naming service is on port 19081.

The example below is taken from the [samples/OcelotServiceFabric](#) folder so please check it if this doesn't make sense!

```
{
  "Routes": [
    {
      "DownstreamScheme": "http",
      "DownstreamPathTemplate": "/api/values",
      "UpstreamPathTemplate": "/EquipmentInterfaces",
      "UpstreamHttpMethod": [ "Get" ],
      "ServiceName": "OcelotServiceApplication/OcelotApplicationService"
    }
  ],
  "GlobalConfiguration": {
    "RequestIdKey": "OcRequestId",
    "ServiceDiscoveryProvider": {
      "Host": "localhost",
      "Port": 19081,
      "Type": "ServiceFabric"
    }
  }
}
```

If you are using stateless / guest exe services, Ocelot will be able to proxy through the naming service without anything else. However, if you are using statefull / actor services, you must send the **PartitionKind** and **PartitionKey** query string values with the client request e.g.

GET <http://ocelot.com/EquipmentInterfaces?PartitionKind=xxx&PartitionKey=xxx>

There is no way for Ocelot to work these out for you.



## TRACING

This page details how to perform distributed tracing with Ocelot.

### 29.1 OpenTracing

Ocelot provides tracing functionality from the excellent [OpenTracing API for .NET](#) project. The code for the Ocelot integration can be found in [Ocelot.Tracing.OpenTracing](#) project.

The example below uses [C# Client for Jaeger](#) client to provide the tracer used in Ocelot. In order to add [OpenTracing](#) services we must call the `AddOpenTracing()` extension of the `OcelotBuilder` being returned by `AddOcelot()`<sup>1</sup> like below:

```
services.AddSingleton<ITracer>(sp =>
{
    var loggerFactory = sp.GetService<ILoggerFactory>();
    Configuration config = new Configuration(context.HostingEnvironment.ApplicationName,
    loggerFactory);

    var tracer = config.GetTracer();
    GlobalTracer.Register(tracer);
    return tracer;
});

services
    .AddOcelot()
    .AddOpenTracing();
```

Then in your **ocelot.json** add the following to the Route you want to trace:

```
"HandlerOptions": {
  "UseTracing": true
}
```

Ocelot will now send tracing information to [Jaeger](#) when this Route is called.

---

<sup>1</sup> The `AddOcelot` method adds default ASP.NET services to DI-container. You could call another more extended `AddOcelotUsingBuilder` method while configuring services to build and use custom builder via an `IMvcCoreBuilder` interface object. See more instructions in [Dependency Injection](#), “[The AddOcelotUsingBuilder method](#)” section.

### 29.1.1 OpenTracing Status

The [OpenTracing](#) project was archived on January 31, 2022 (see [the article](#)). The Ocelot team will decide on a migration to [OpenTelemetry](#) which is highly desired.

## 29.2 Butterfly

Ocelot provides tracing functionality from the excellent [Butterfly](#) project. The code for the Ocelot integration can be found in [Ocelot.Tracing.Butterfly](#) project.

In order to use the tracing please read the [Butterfly](#) documentation.

In Ocelot you need to add the [NuGet package](#) if you wish to trace a Route:

**Install-Package** Ocelot.Tracing.Butterfly

In your `ConfigureServices` method to add Butterfly services: we must call the `AddButterfly()` extension of the `OcelotBuilder` being returned by `AddOcelot()`<sup>[Page 93, 1](#)</sup> like below:

```
services
    .AddOcelot()
    // This comes from Ocelot.Tracing.Butterfly package
    .AddButterfly(option =>
    {
        // This is the URL that the Butterfly collector server is running on...
        option.CollectorUrl = "http://localhost:9618";
        option.Service = "Ocelot";
    });
```

Then in your `ocelot.json` add the following to the Route you want to trace:

```
"HandlerOptions": {
  "UseTracing": true
}
```

Ocelot will now send tracing information to Butterfly when this Route is called.

---

## WEBSOCKETS

[WebSockets Standard](#) by WHATWG organization

Ocelot supports proxying [WebSockets](#) with some extra bits. This functionality was requested in [issue 212](#).

In order to get *WebSocket* proxying working with Ocelot you need to do the following. In your `Configure` method you need to tell your application to use *WebSockets*:

```
Configure(app =>
{
    app.UseWebSockets();
    app.UseOcelot().Wait();
})
```

Then in your `ocelot.json` add the following to proxy a Route using *WebSockets*:

```
{
  "UpstreamPathTemplate": "/",
  "DownstreamPathTemplate": "/ws",
  "DownstreamScheme": "ws",
  "DownstreamHostAndPorts": [
    { "Host": "localhost", "Port": 5001 }
  ]
}
```

With this configuration set Ocelot will match any *WebSocket* traffic that comes in on / and proxy it to `localhost:5001/ws`. To make this clearer Ocelot will receive messages from the upstream client, proxy these to the downstream service, receive messages from the downstream service and proxy these to the upstream client.

### 30.1 Links

- WHATWG: [WebSockets Standard](#)
- Mozilla Developer Network: [The WebSocket API \(WebSockets\)](#)
- Microsoft Learn: [WebSockets support in ASP.NET Core](#)
- Microsoft Learn: [WebSockets support in .NET](#)

## 30.2 SignalR

Welcome to [Real-time ASP.NET with SignalR](#)

Ocelot supports proxying *SignalR*. This functionality was requested in [issue 344](#). In order to get *WebSocket* proxying working with Ocelot you need to do the following.

**First**, install [SignalR Client](#) NuGet package:

```
NuGet\Install-Package Microsoft.AspNetCore.SignalR.Client
```

The package is deprecated, but [new versions](#) are still built from the source code. So, SignalR is [the part](#) of the ASP.NET Framework which can be referenced like:

```
<ItemGroup>
  <FrameworkReference Include="Microsoft.AspNetCore.App" />
</ItemGroup>
```

More information on framework compatibility can be found in instructions: [Use ASP.NET Core APIs in a class library](#).

**Second**, you need to tell your application to use *SignalR*. Complete reference is here: [ASP.NET Core SignalR configuration](#)

```
public void ConfigureServices(IServiceCollection services)
{
    services.AddOcelot();
    services.AddSignalR();
}
```

Pay attention to configuration of transport level of *WebSockets*, so [configure allowed transports](#) to allow *WebSockets* connections.

**Then** in your **ocelot.json** add the following to proxy a Route using SignalR. Note normal Ocelot routing rules apply the main thing is the scheme which is set to **ws**.

```
{
  "UpstreamHttpMethod": [ "GET", "POST", "PUT", "DELETE", "OPTIONS" ],
  "UpstreamPathTemplate": "/gateway/{catchAll}",
  "DownstreamPathTemplate": "/{catchAll}",
  "DownstreamScheme": "ws",
  "DownstreamHostAndPorts": [
    { "Host": "localhost", "Port": 5001 }
  ]
}
```

## 30.3 Supported

1. *Load Balancer*
2. *Routing*
3. *Service Discovery*

This means that you can set up your downstream services running *WebSockets* and either have multiple **DownstreamHostAndPorts** in your Route config, or hook your Route into a service discovery provider and then load balance requests... Which we think is pretty cool.

## 30.4 Not Supported

Unfortunately a lot of Ocelot features are non *WebSocket* specific, such as header and http client stuff. We have listed what will not work below:


1. *Tracing*
2. *Request ID*
3. *Request Aggregation*
4. *Rate Limiting*
5. *Quality of Service*
6. *Middleware Injection*
7. *Headers Transformation*
8. *Delegating Handlers*
9. *Claims Transformation*
10. *Caching*
11. *Authentication*<sup>1</sup>
12. *Authorization*

We are not 100% sure what will happen with this feature when it gets into the wild, so please make sure you test thoroughly!

## 30.5 Future

*Websockets* and *SignalR* are being developed intensively by the .NET community, so you need to watch for trends, releases in official docs regularly:

- [WebSockets docs](#)
- [SignalR docs](#)

As a team, we cannot advise you on development, but feel free to ask questions, get coding recipes in the [Discussions](#) space of the repository. 

Also, we welcome any bug reports, enhancements or proposals regarding this feature.

The Ocelot team considers the current implementation of WebSockets feature obsolete, based on the [WebSocketsProxyMiddleware](#) class. Websockets are the part of ASP.NET Core framework having native [WebSocketMiddleware](#) class. We have a strong intention to migrate or at least redesign the feature, see [issue 1707](#).

---

<sup>1</sup> If anyone requests it, we might be able to do something with basic authentication.





## OVERVIEW

This document summarises the build and release process for the project. The build scripts are written using [Cake](#), and they are defined in `./build.cake`. The scripts have been designed to be run by either developers locally or by a build server (currently [CircleCi](#)), with minimal logic defined in the build server itself.



## BUILDING

- You can also just run `dotnet tool restore && dotnet cake` locally! Output will go to the `./artifacts` directory.
- The best way to replicate the CI process is to build Ocelot locally is using the `Dockerfile.build` file which can be found in the `docker` folder in `Ocelot` root. Use the following command `docker build --platform linux/amd64 -f ./docker/Dockerfile.build .` for example. You will need to change the platform flag depending on your platform.
- There is a `Makefile` to make it easier to call the various targets in `build.cake`. The scripts are called with `.sh` but can be easily changed to `.ps1` if you are using Windows.
- Alternatively you can build the project in VS2022 with the latest `.NET 8.0` SDK.



The tests should all just run and work as part of the build process. You can of course also run them in Visual Studio.

## 33.1 Create SSL Cert for Testing

You can do this via [OpenSSL](#):

- Install [openssl package](#) (if you are using Windows, download binaries [here](#)).
- Generate private key: `openssl genrsa 2048 > private.pem`
- Generate the self-signed certificate: `openssl req -x509 -days 1000 -new -key private.pem -out public.pem`
- If needed, create PFX: `openssl pkcs12 -export -in public.pem -inkey private.pem -out mycert.pfx`



## RELEASE PROCESS

- The release process works best with [Gitflow](#) branching.
- Contributors can do whatever they want on PRs and feature branches to deliver a feature to **develop** branch.
- Maintainers can do whatever they want on PRs and merges to **main** will result in packages being released to GitHub and NuGet.

Ocelot uses the following process to accept work into the NuGet packages.

1. User creates an issue or picks up an [existing issue](#) in GitHub. An issue can be created by converting [discussion](#) topics if necessary and agreed upon.
2. User creates a [fork](#) and branches from this (unless a member of core team, they can just create a branch on the head repo) e.g. `feature/xxx`, `bug/xxx` etc. It doesn't really matter what the "xxx" is. It might make sense to use the issue number and maybe a short description.
3. When the contributor is happy with their work they can create a pull request against **develop** in GitHub with their changes.
4. The maintainer must follow the [SemVer](#) support for this is provided by [GitVersion](#). So if the maintainer needs to make breaking changes, be sure to use the correct commit message, so **GitVersion** uses the correct **SemVer** tags. Do not manually tag the Ocelot repo: this will break things!
5. The Ocelot team will review the PR and if all is good merge it, else they will suggest feedback that the user will need to act on.

In order to speed up getting a PR the contributor should think about the following:

- Have I covered all my changes with tests at unit and acceptance level?
- Have I updated any documentation that my changes may have affected?
- Does my feature make sense, have I checked all of Ocelot's other features to make sure it doesn't already exist?

In order for a PR to be merged the following must have occurred:

- All new code is covered by unit tests.
  - All new code has at least 1 acceptance test covering the happy path.
  - Tests must have passed locally.
  - Build must have green status.
  - Build must not have slowed down dramatically.
  - The main Ocelot package must not have taken on any non MS dependencies.
6. After the PR is merged to **develop** the Ocelot NuGet packages will not be updated until a release is created.

7. When enough work has been completed to justify a new release, **develop** branch will be merged into **main** as **release/xxx** branch, the release process will begin which builds the code, versions it, pushes artifacts to GitHub and NuGet packages to NuGet.
8. The final step is to go back to GitHub and close any issues that are now fixed. **Note:** All linked issues to the PR in **Development** settings (right side PR settings) will be closed automatically while merging the PR. It is imperative that developer uses the “**Link an issue from this repository**” pop-up dialog of the **Development** settings!

### 34.1 Notes

All NuGet package builds and releases are done with CircleCI, see [Pipelines - ThreeMammals/Ocelot](#).

Only Tom Pallister (owner) and Ocelot Core Team members (maintainers) can merge releases into **main** at the moment. This is to ensure there is a final *quality gate* in place. Tom is mainly looking for security issues on the final merge.

We **do** follow this development and release process! If anything is unclear or you get stuck in the process, please contact the [Ocelot Core Team](#) members or repository maintainers.

### 34.2 Quality Gates

To be developed...