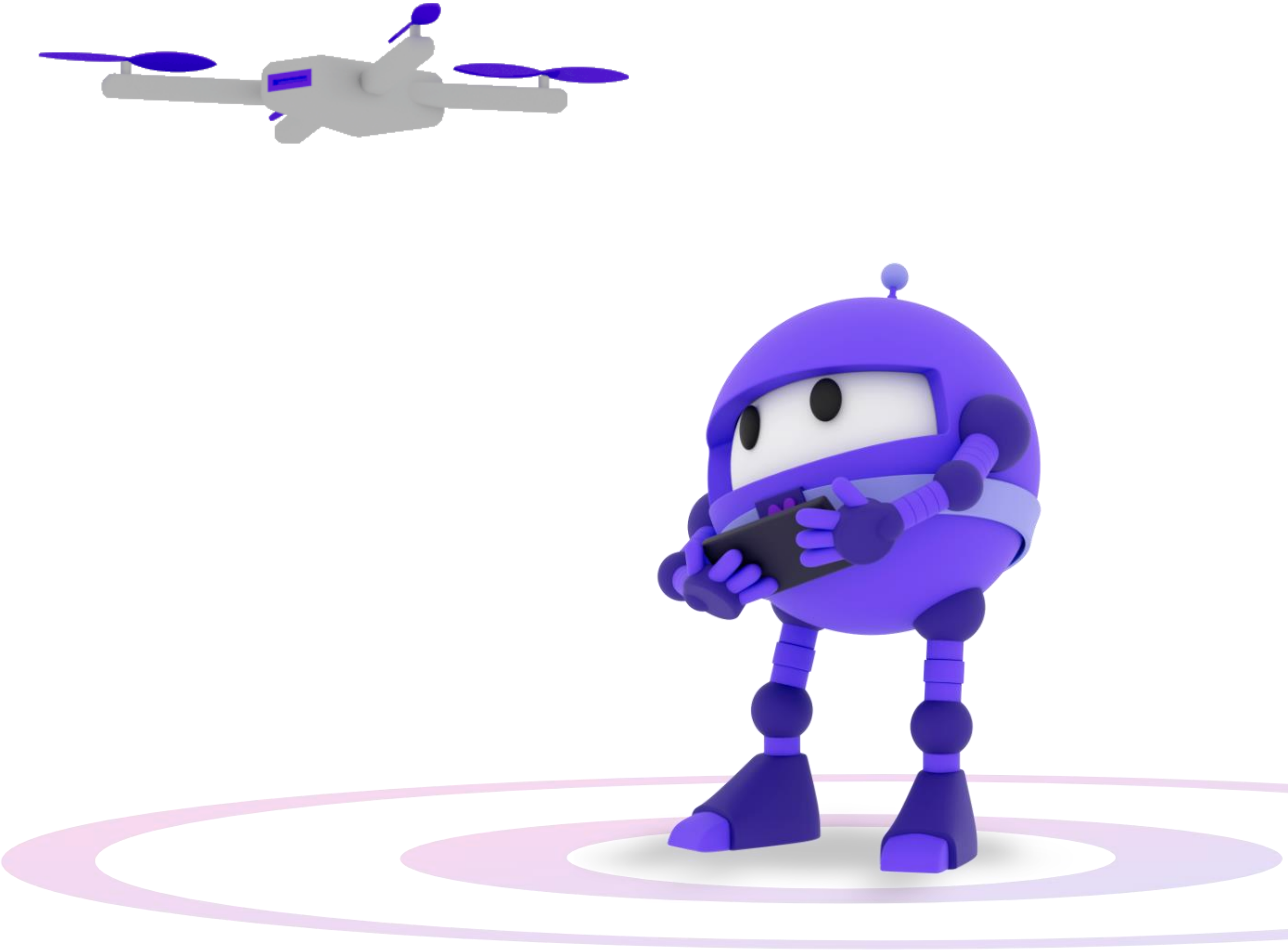
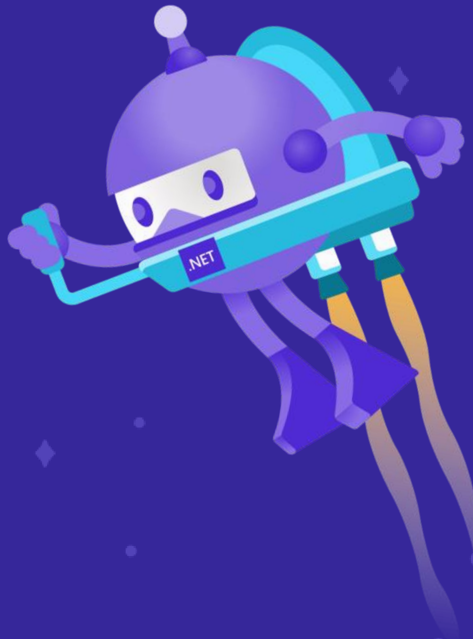
.NET Conf 2023
x Seoul



Identity and Access Management for your web app

Mats Lundell-Nygjelten



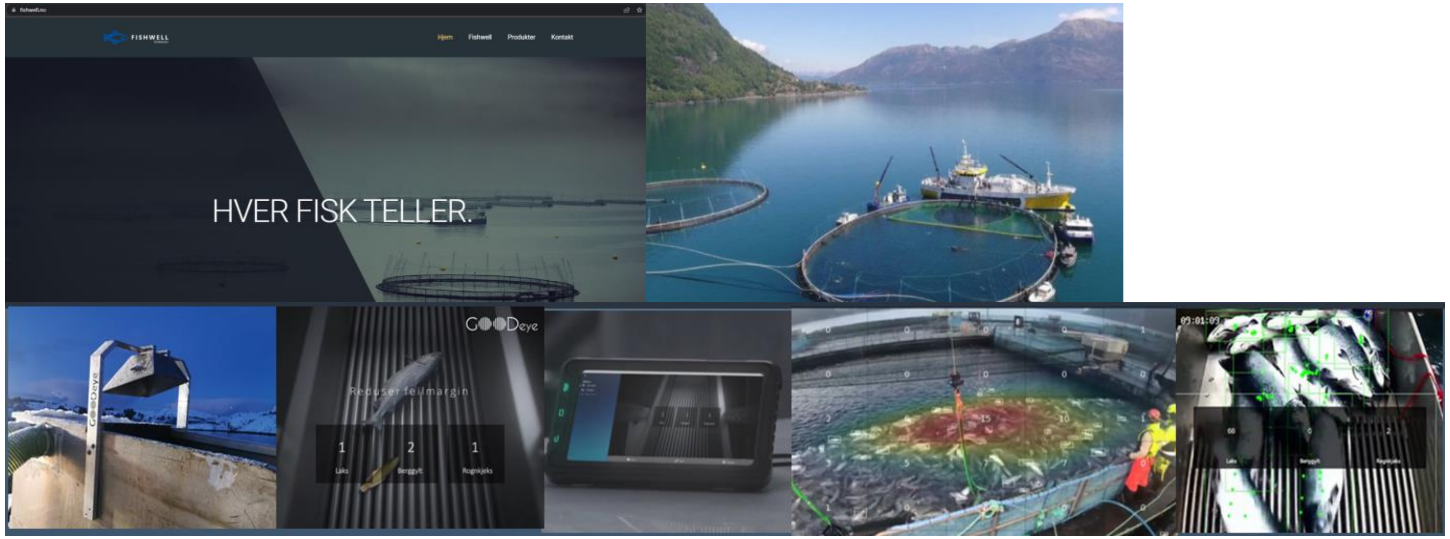
Introduction

- Mats Lundell-Nygjelten
- Norway
- Solution Architect
- Fish farming
- Fishwell Technology

React

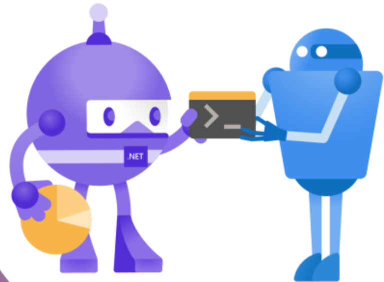
C#

Azure



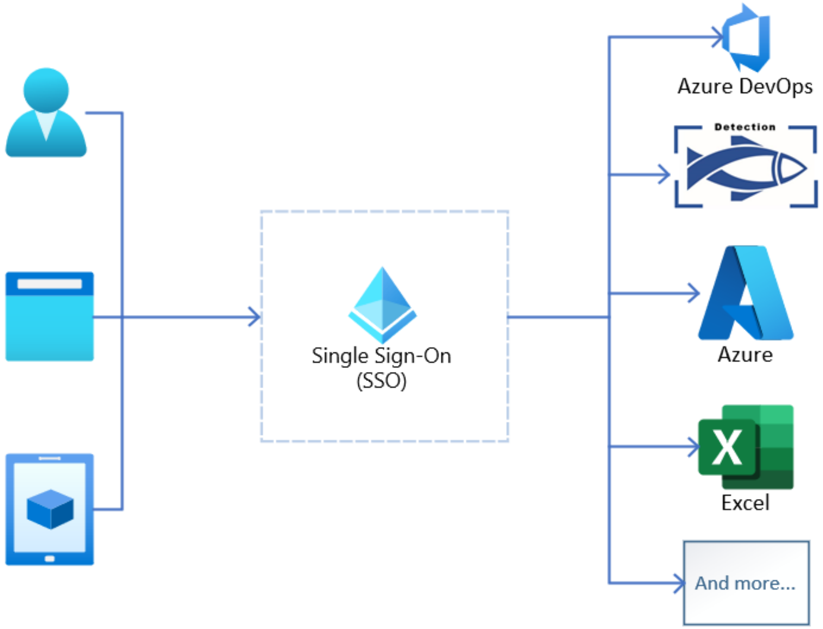
Agenda

1. A few definitions – make sure we are on the same page
2. Why do you need an enterprise level identity and access management tool?
3. Use our experience to link theory to a real-world example
4. Type of users
5. Access Management with Tenants and Roles

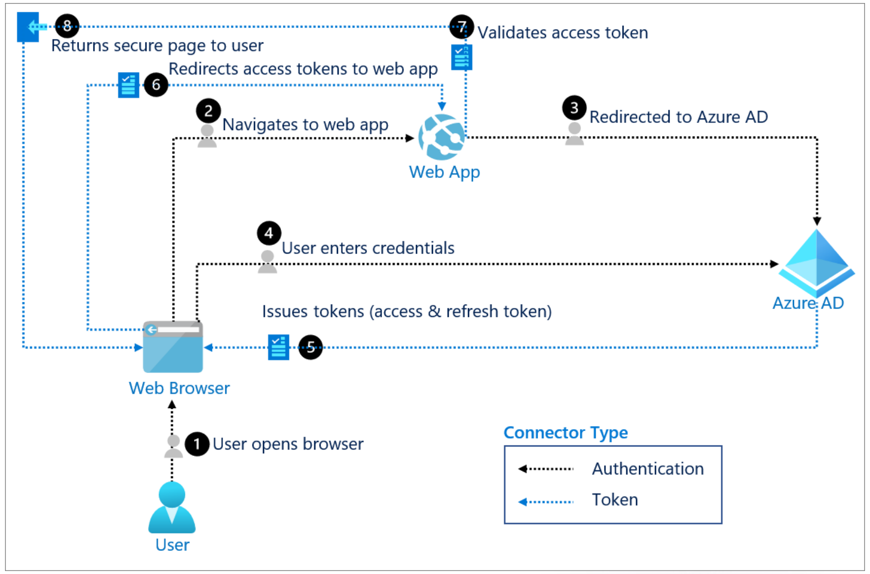


Single Sign-On (SSO)

- Single sign-on is an authentication method that allows users to sign in using one set of credentials to multiple independent software systems.
- Using SSO means a user doesn't have to sign into every application they use.



OAuth 2.0 and OpenID Connect (OIDC)



OAuth 2.0

The OAuth 2.0 is the industry protocol for authorization. It allows a user to grant limited access to its protected resources. Designed to work specifically with Hypertext Transfer Protocol (HTTP), OAuth separates the role of the client from the resource owner.

OAuth 2.0 is directly related to OpenID Connect (OIDC)

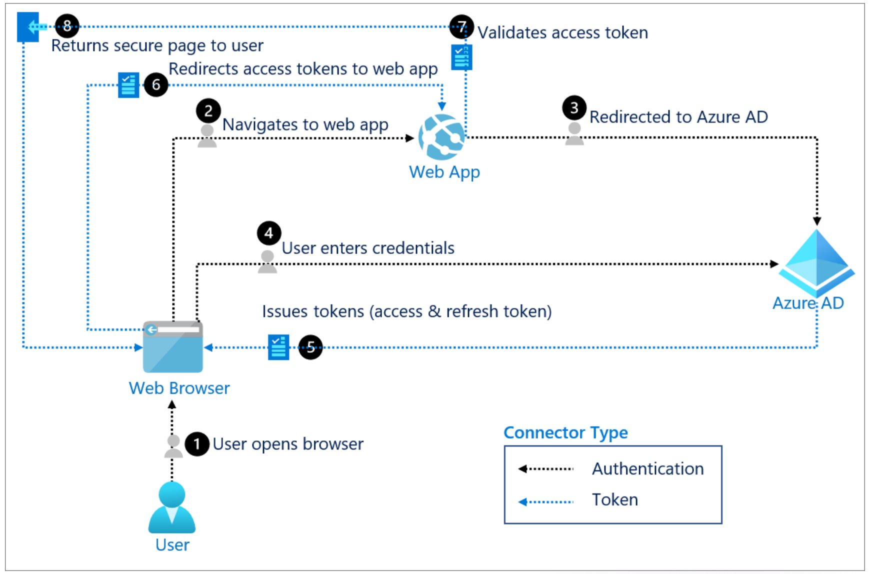
OpenID Connect

OpenID Connect (OIDC) extends the OAuth 2.0 authorization protocol for use also as an authentication protocol. You can use OIDC to enable single sign-on (SSO) between your OAuth-enabled applications by using a security token called an ID token.

The full specification for OIDC is available on the OpenID Foundation's website at OpenID Connect Core 1.0 specification.

https://openid.net/specs/openid-connect-core-1_0.html

OAuth 2.0 and OpenID Connect (OIDC)



OAuth 2.0

ACCESS TOKEN

OpenID Connect

ID TOKEN

https://openid.net/specs/openid-connect-core-1_0.html

Azure Active Directory (AAD) and Multitenancy

Azure Active Directory

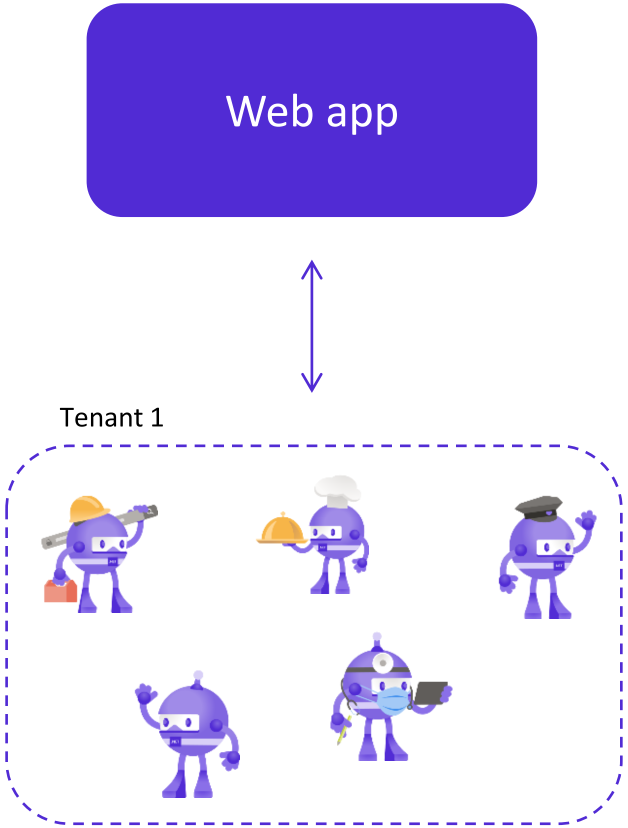
Azure Active Directory is a cloud service that provides administrators with the ability to manage end-user identities and access privileges. Its services include core directory, access management and identity protection

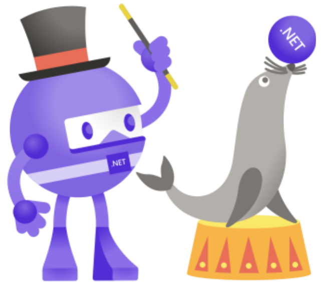
Multitenancy

A tenant is a group of users. In a SaaS application, the tenant is a subscriber or customer of the application. Multitenancy is an architecture where multiple tenants share the same physical instance of the app.

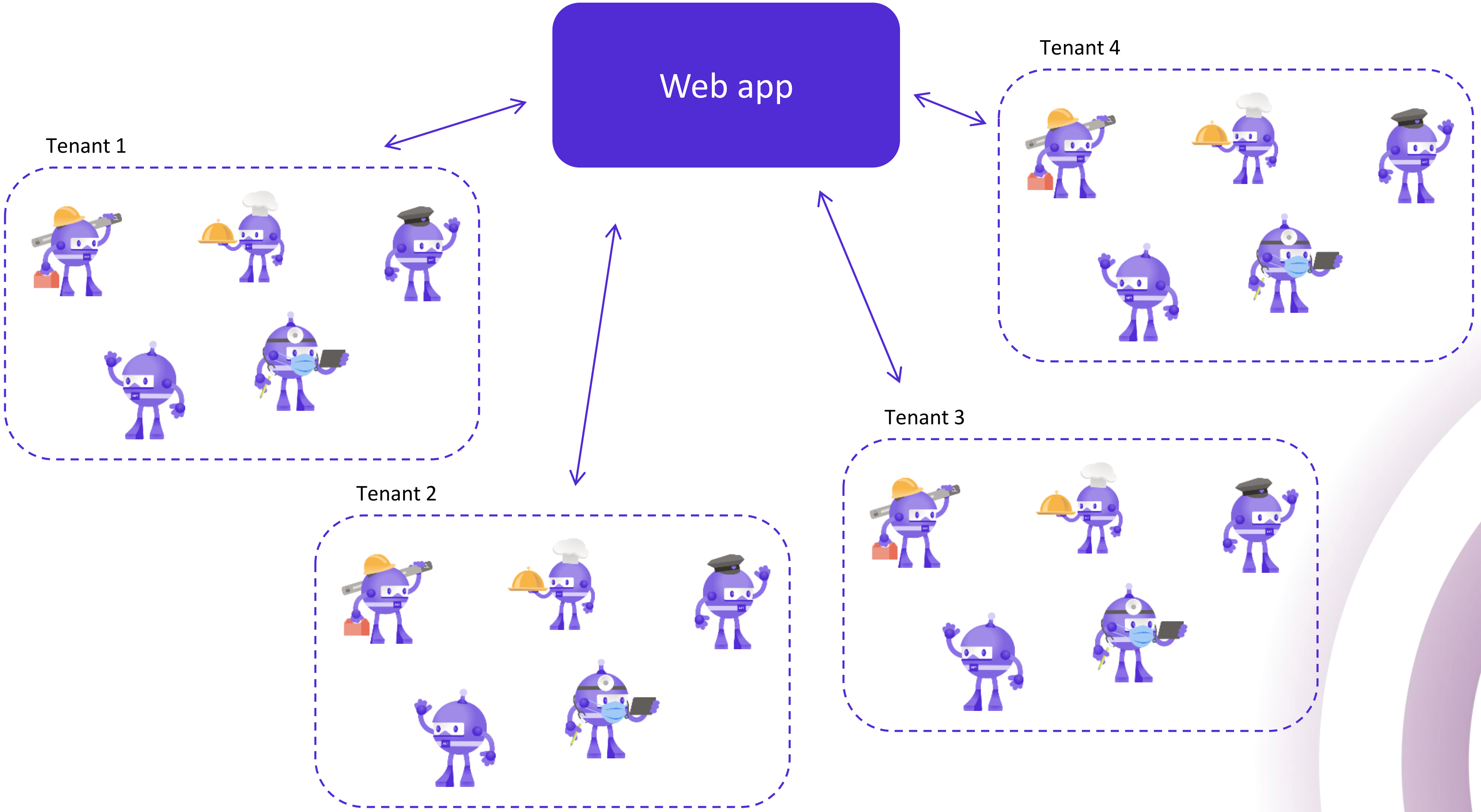
Although tenants share physical resources (such as VMs or storage), each tenant gets its own logical instance of the app.

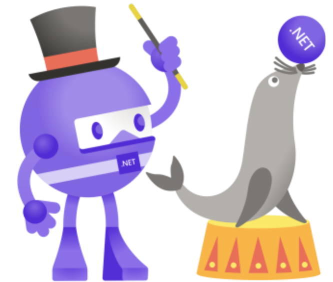
Single tenant web app



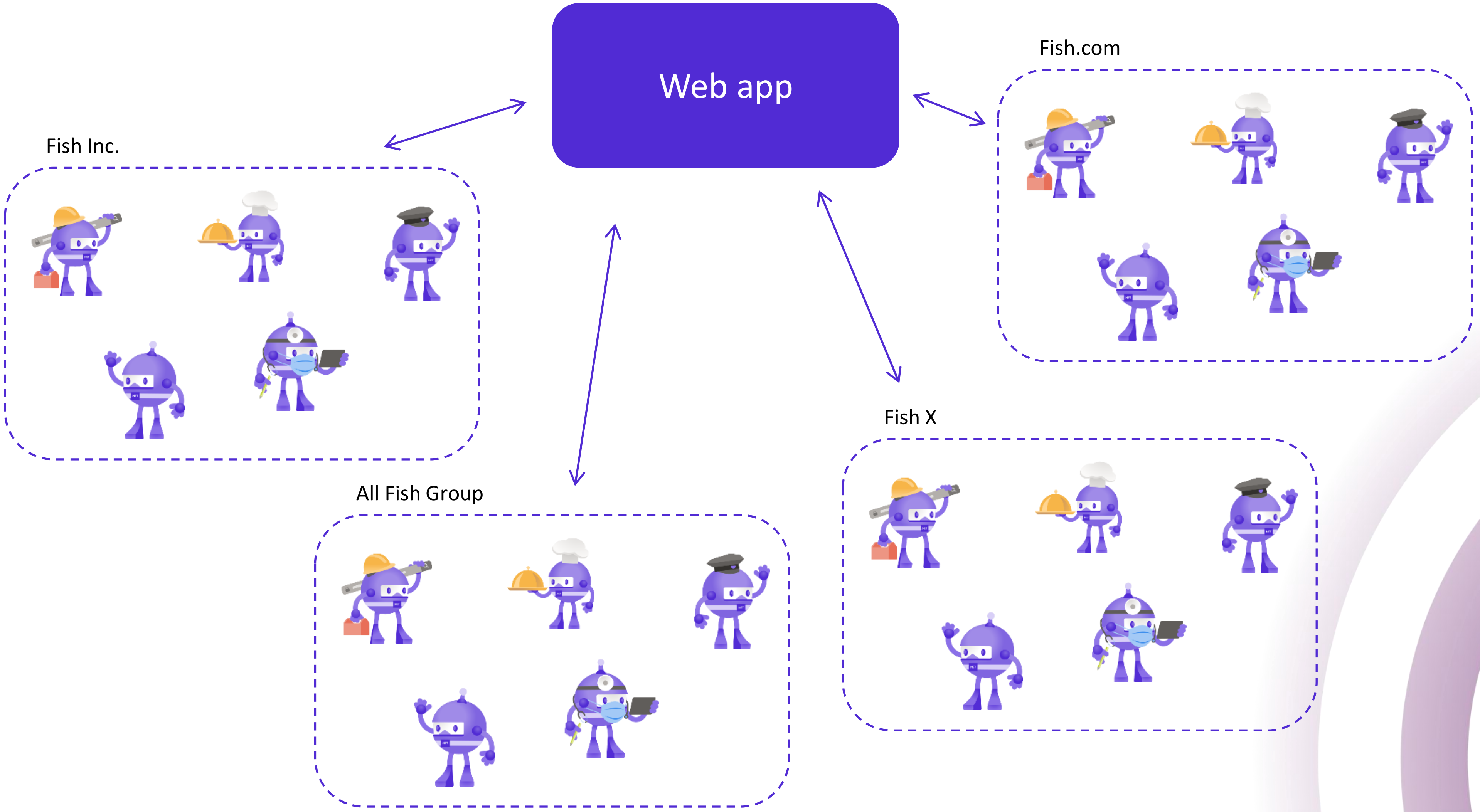


Multitenant web app





Multitenant web app



Web app

Fish Inc.

Fish.com

All Fish Group

Fish X

Identity and Access Management Tool

Customers of your service need

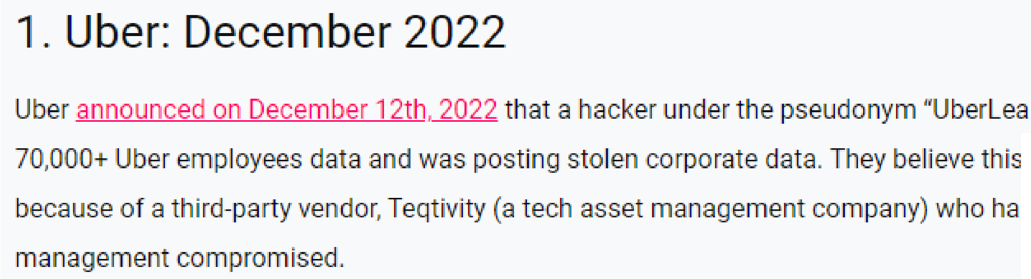
1. Their own account
2. Be able to login
3. Manage their own data
4. Access to functionality linked to their role

Data management

- Customer trust
- Strict control

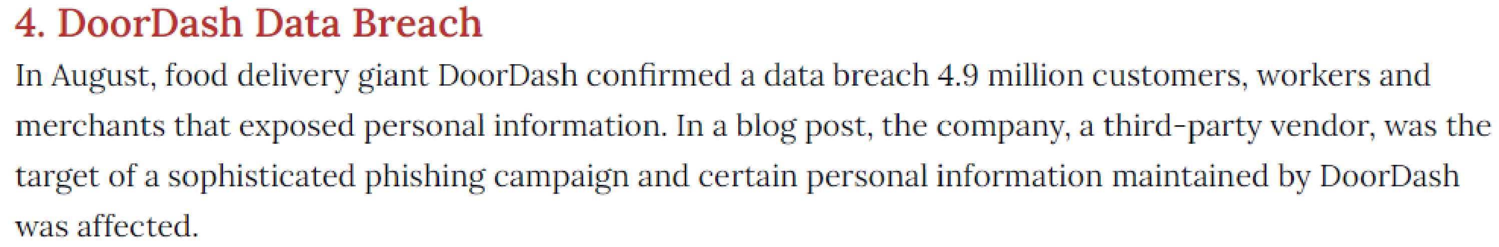
We need a secure solution – we don’t want to be the next headline in the newspaper…

Examples of user information getting leaked



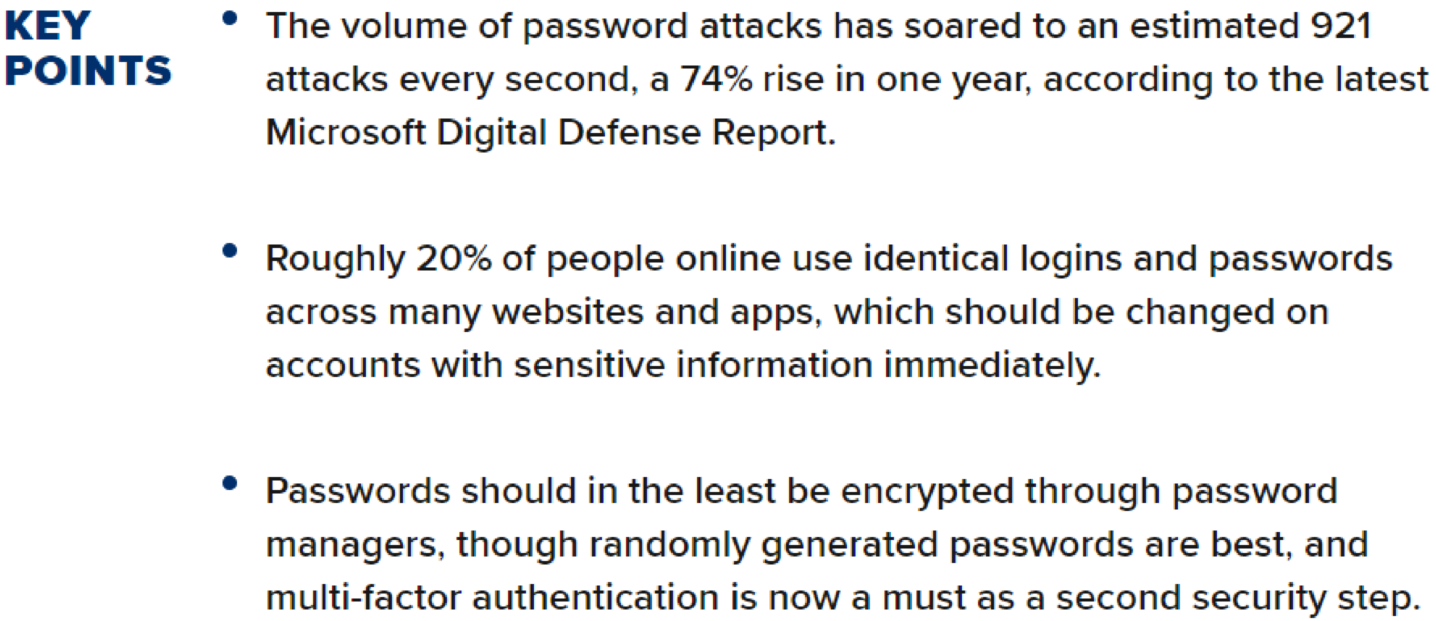
1. Uber: December 2022

Uber announced on December 12th, 2022 that a hacker under the pseudonym "UberLeaks" gained access to 70,000+ Uber employees data and was posting stolen corporate data. They believe this because of a third-party vendor, Teqtivity (a tech asset management company) who ha management compromised.



4. DoorDash Data Breach

In August, food delivery giant DoorDash confirmed a data breach 4.9 million customers, workers and merchants that exposed personal information. In a blog post, the company, a third-party vendor, was the target of a sophisticated phishing campaign and certain personal information maintained by DoorDash was affected.

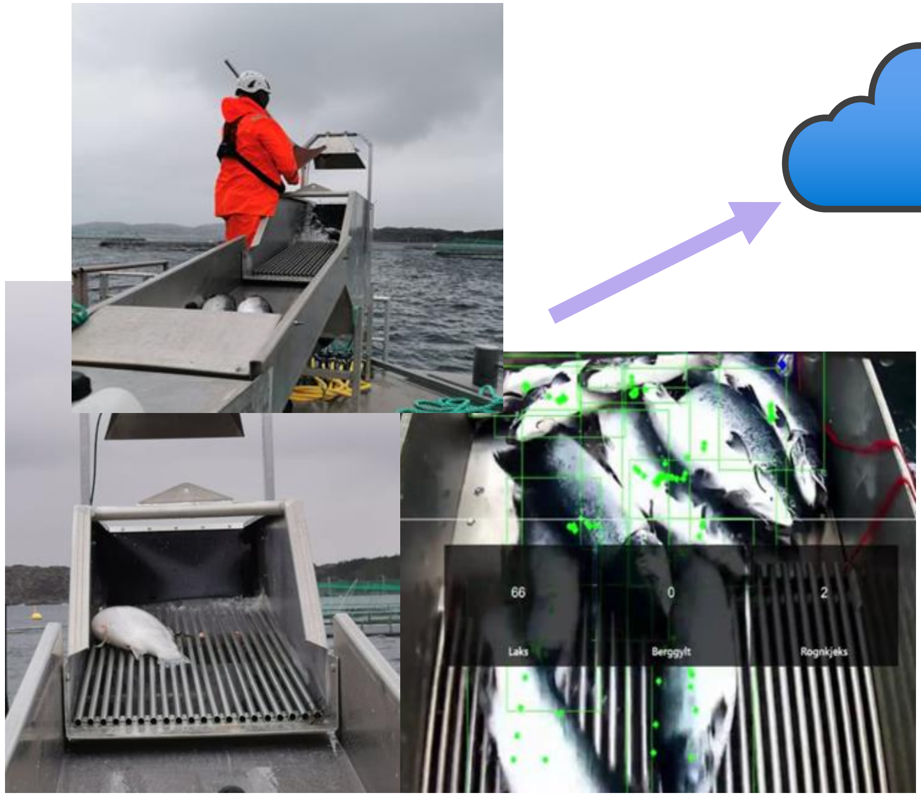


KEY POINTS

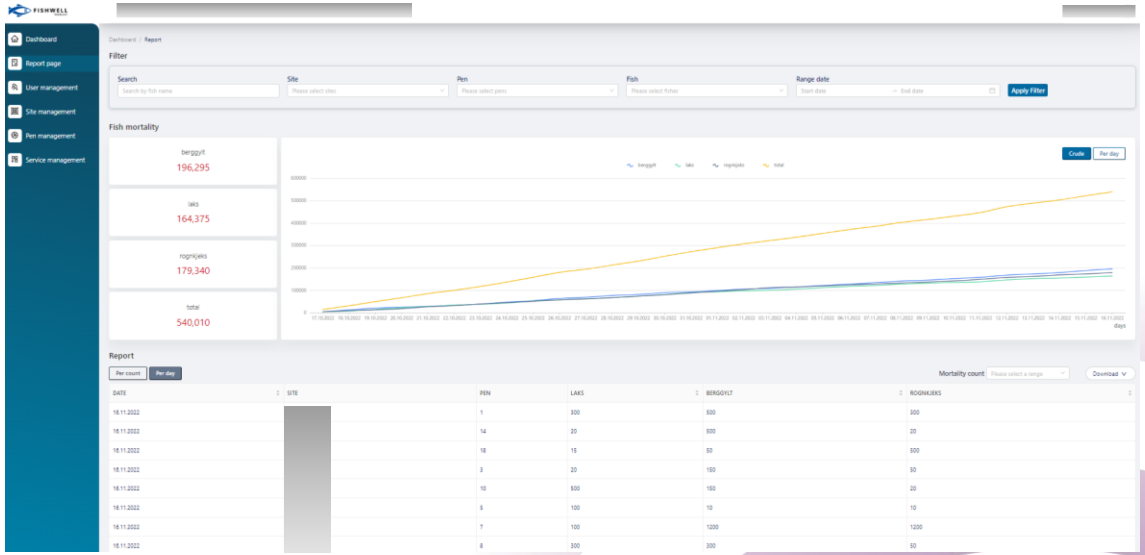
- The volume of password attacks has soared to an estimated 921 attacks every second, a 74% rise in one year, according to the latest Microsoft Digital Defense Report.
- Roughly 20% of people online use identical logins and passwords across many websites and apps, which should be changed on accounts with sensitive information immediately.
- Passwords should in the least be encrypted through password managers, though randomly generated passwords are best, and multi-factor authentication is now a must as a second security step.

https://www.electric.ai/blog/recent-big-company-data-breaches
https://www.securitymagazine.com/articles/98716-the-top-10-data-breaches-of-2022
https://www.cnbc.com/2022/11/21/why-microsofts-hack-data-means-you-may-need-new-login-passwords.html

Our dead fish counter - Fishwell Detection



detection.fishwell.no



[redacted]

[redacted]

Dashboard / Report

Filter

Search: Search by fish name

Site: Please select sites

Pen: Please select pens

Fish: Please select fishes

Range date: Start date → End date

Apply Filter

Fish mortality

berggylt
196,295

laks
164,375

rognkjeks
179,340

total
540,010

Report

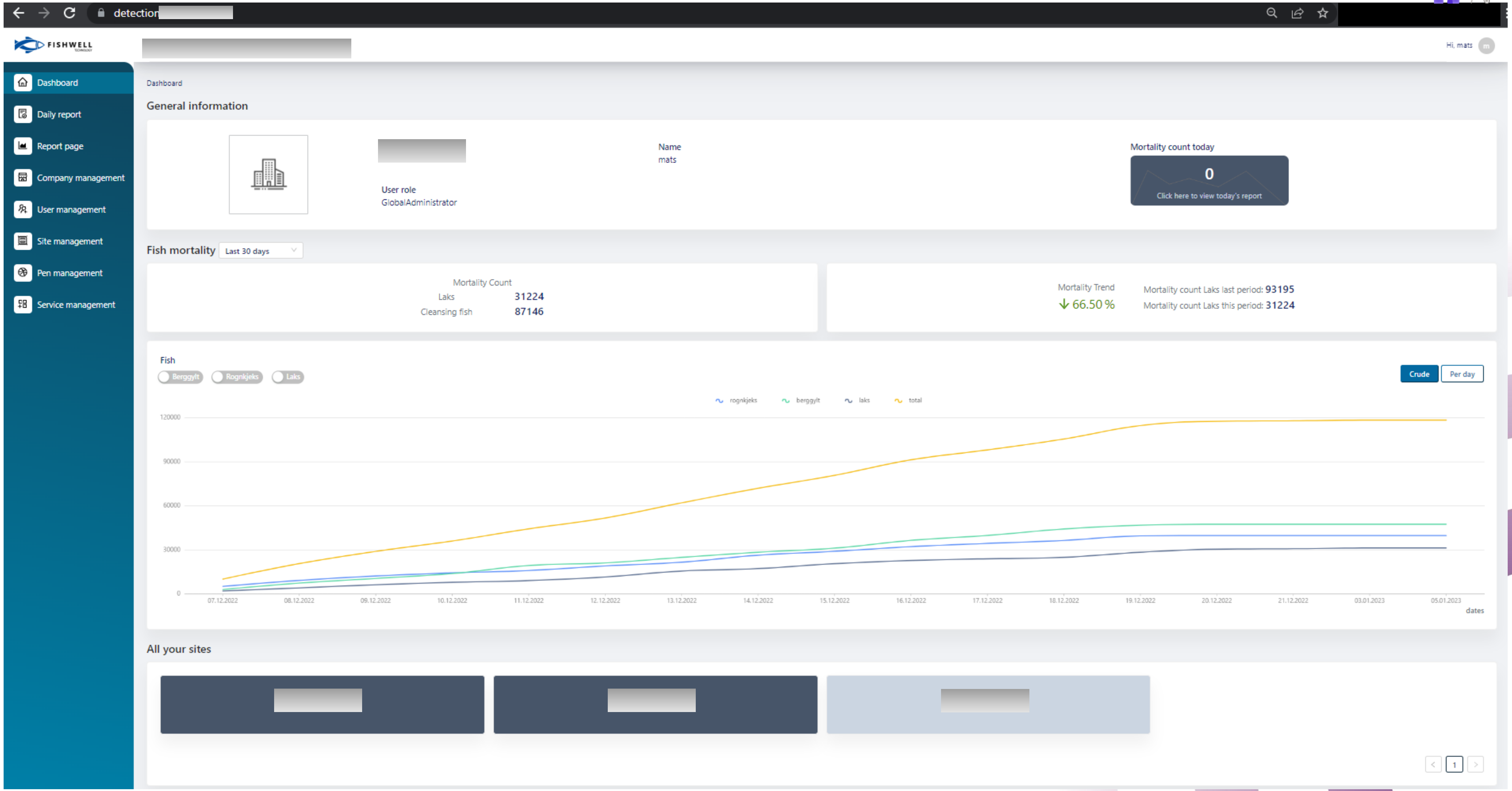
Per count | Per day

Mortality count: Please select a range

Download

DATE	SITE	PEN	LAKS	BERGGYLT	ROGNKJEKS
16.11.2022	[redacted]	1	300	500	300
16.11.2022	[redacted]	14	20	500	20
16.11.2022	[redacted]	18	15	50	500
16.11.2022	[redacted]	3	20	150	50
16.11.2022	[redacted]	10	500	150	20
16.11.2022	[redacted]	5	100	10	10
16.11.2022	[redacted]	7	100	1200	1200
16.11.2022	[redacted]	8	300	300	50

Our dead fish counter - Fishwell Detection



Dashboard

General information

[redacted]

User role
GlobalAdministrator

Name
mats

Mortality count today
0
Click here to view today's report

Fish mortality Last 30 days

Mortality Count

Laks	31224
Cleansing fish	87146

Mortality Trend
↓ 66.50 %

Mortality count Laks last period: 93195
Mortality count Laks this period: 31224

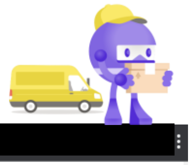
All your sites

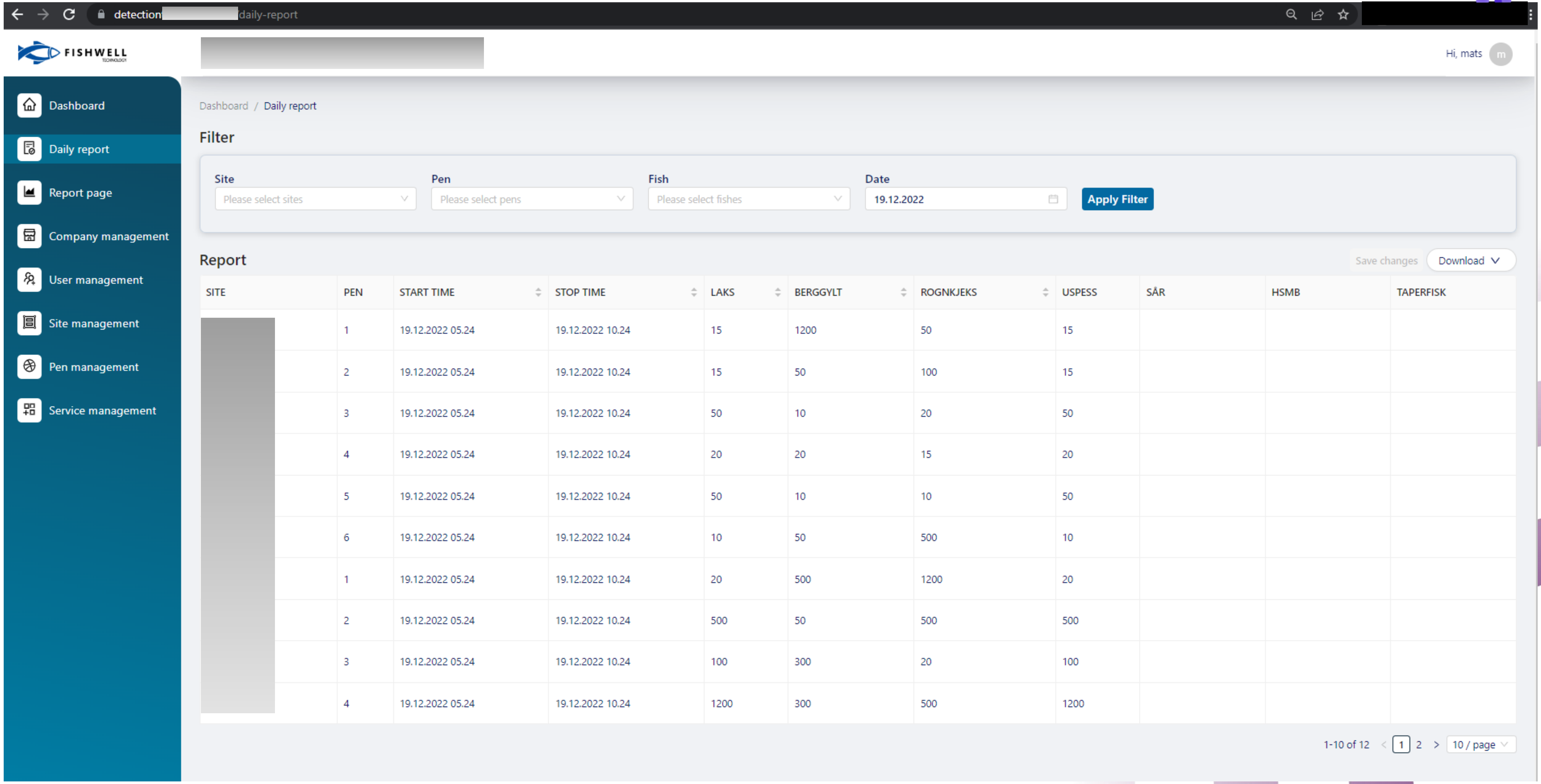
[redacted]

[redacted]

[redacted]

Our dead fish counter - Fishwell Detection





Dashboard / Daily report

Filter

Site: Please select sites

Pen: Please select pens

Fish: Please select fishes

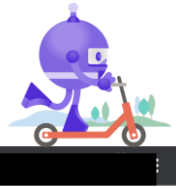
Date: 19.12.2022

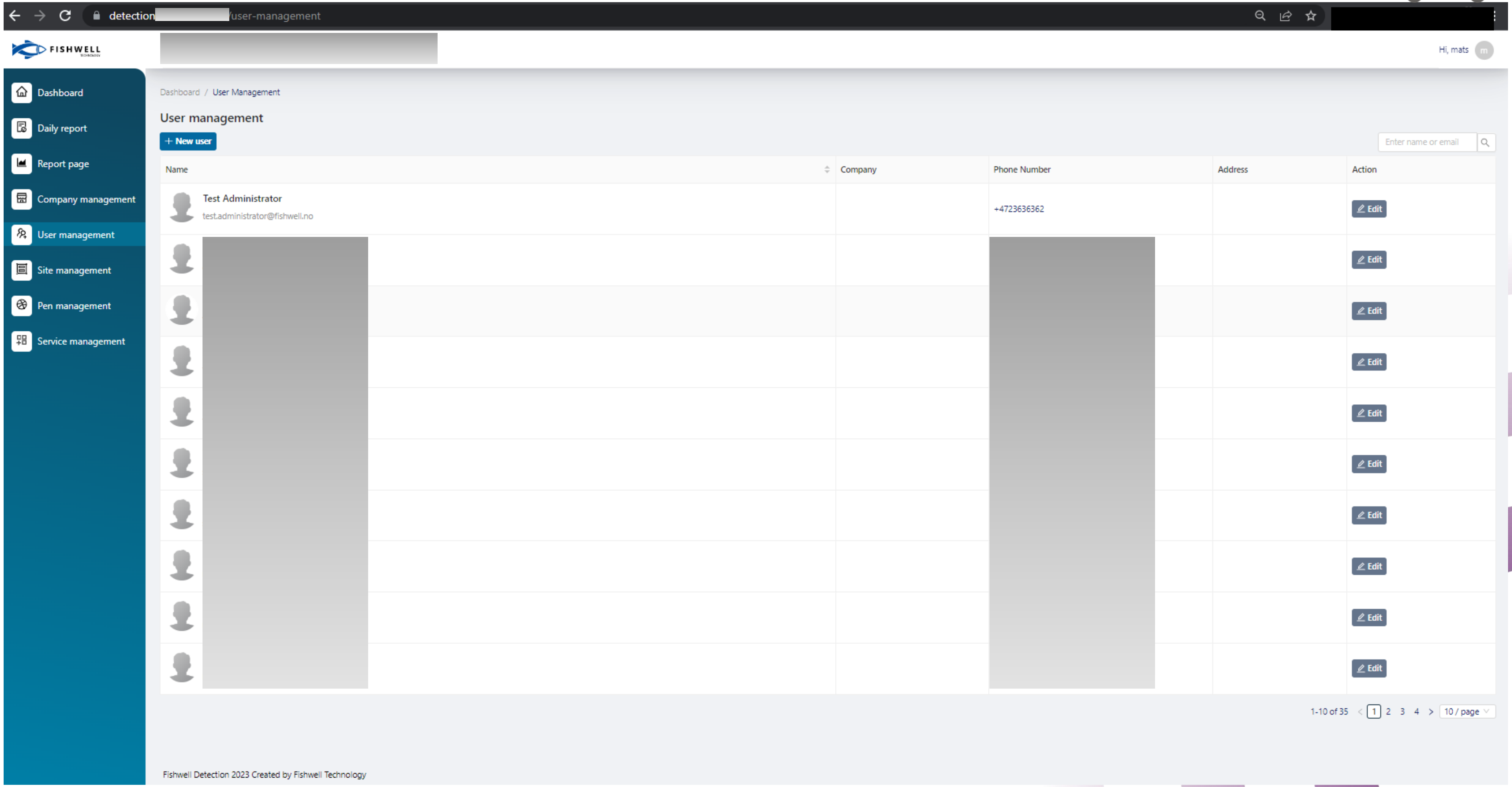
Apply Filter

Report

SITE	PEN	START TIME	STOP TIME	LAKS	BERGGYLT	ROGNKJEKS	USPESS	SÅR	HSMB	TAPERFISK
[redacted]	1	19.12.2022 05.24	19.12.2022 10.24	15	1200	50	15			
[redacted]	2	19.12.2022 05.24	19.12.2022 10.24	15	50	100	15			
[redacted]	3	19.12.2022 05.24	19.12.2022 10.24	50	10	20	50			
[redacted]	4	19.12.2022 05.24	19.12.2022 10.24	20	20	15	20			
[redacted]	5	19.12.2022 05.24	19.12.2022 10.24	50	10	10	50			
[redacted]	6	19.12.2022 05.24	19.12.2022 10.24	10	50	500	10			
[redacted]	1	19.12.2022 05.24	19.12.2022 10.24	20	500	1200	20			
[redacted]	2	19.12.2022 05.24	19.12.2022 10.24	500	50	500	500			
[redacted]	3	19.12.2022 05.24	19.12.2022 10.24	100	300	20	100			
[redacted]	4	19.12.2022 05.24	19.12.2022 10.24	1200	300	500	1200			

Our dead fish counter - Fishwell Detection





detection[redacted]/user-management [redacted]

[redacted]

Hi, mats

Dashboard / User Management

User management

Name	Company	Phone Number	Address	Action
Test Administrator test.administrator@fishwell.no		+4723636362		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit

1-10 of 35 < 1 2 3 4 > 10 / page

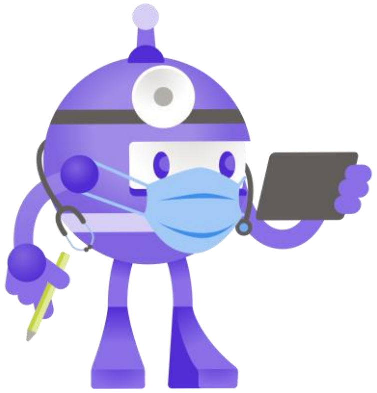
Fishwell Detection 2023 Created by Fishwell Technology

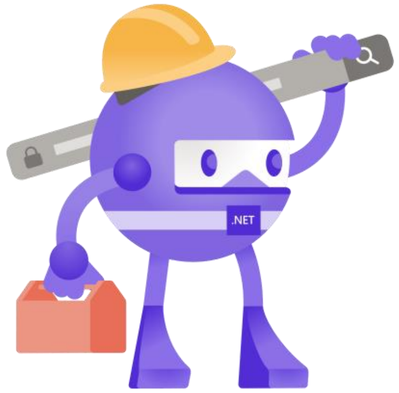
What types of users do we have?

Business-to-business (B2B) solutions, such as accounting software, work tracking, and other software as a service (SaaS) products.

Business-to-consumer (B2C) solutions, such as music streaming, photo sharing, and social network services.

Users within your AAD. A customer that wants to onboard without using their own identity and access management tool.



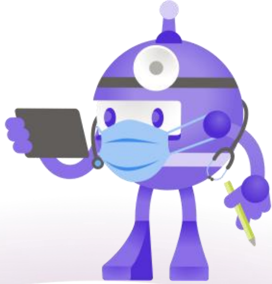


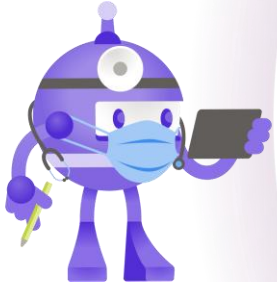
Business-to-business (B2B)

For us B2B customers will be

- Companies from our network of partners
- Fish farming companies

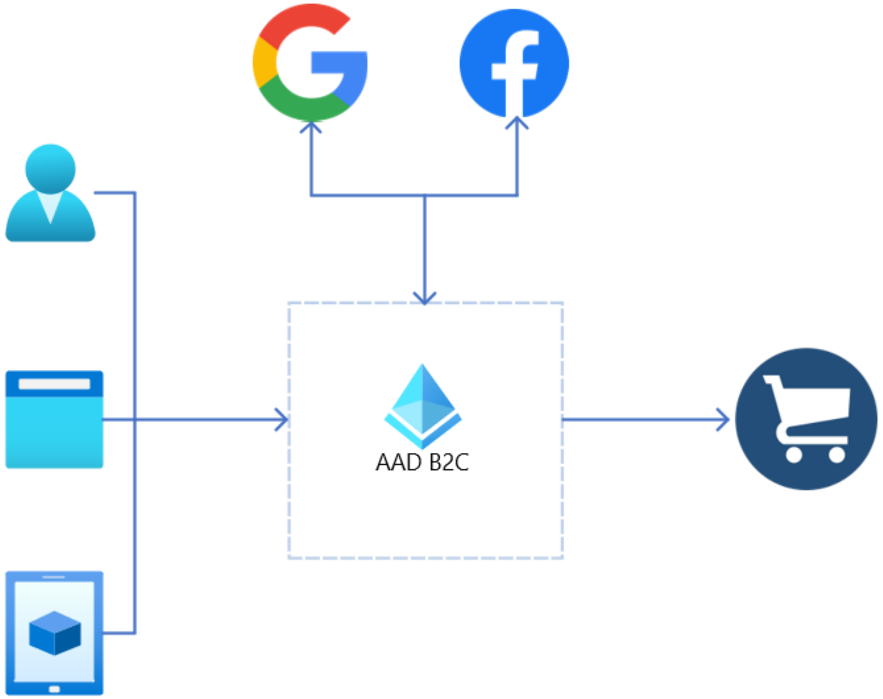
An administrator from their tenant need to sign up to our application for their users to get access





Business-to-consumer (B2C)

We are not using this solution (yet).



Users within our AAD

Our short-term solution if a customer does not have

1. Developers available for integration development
2. Time to wait before testing our services

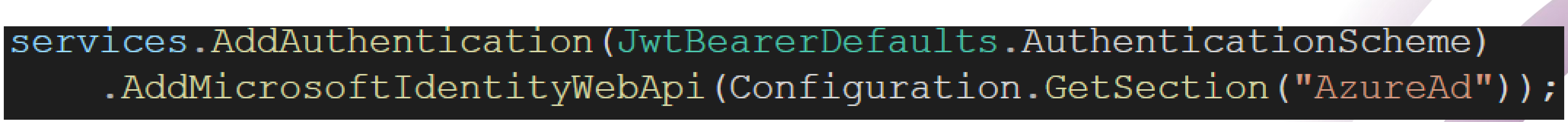
We need a way to add them quickly to our system

First - authentication

Need to configure the authentication middleware in the startup class.

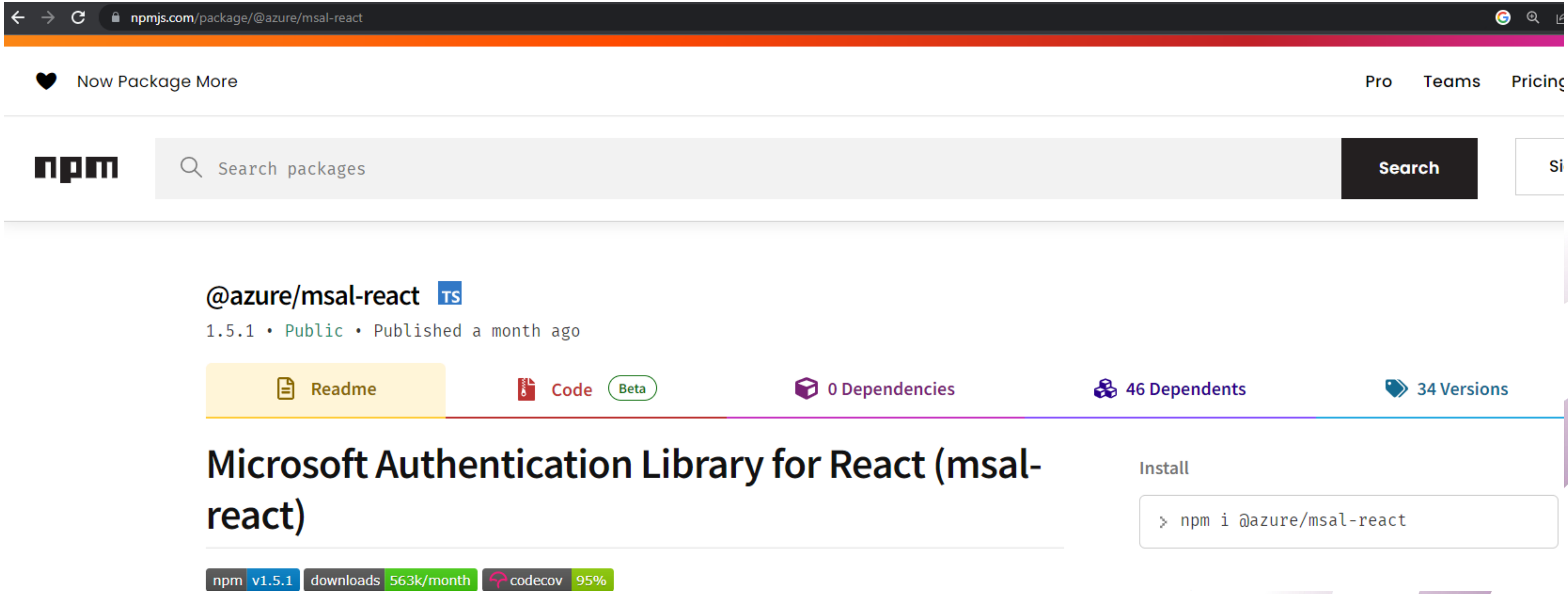
1. Authentication scheme

2. AAD configuration



```
services.AddAuthentication(JwtBearerDefaults.AuthenticationScheme)
    .AddMicrosoftIdentityWebApi(Configuration.GetSection("AzureAd"));
```

First - authentication



npmjs.com/package/@azure/msal-react

Now Package More

Pro Teams Pricing

npm

Search packages

Search

Si

@azure/msal-react

1.5.1 • Public • Published a month ago

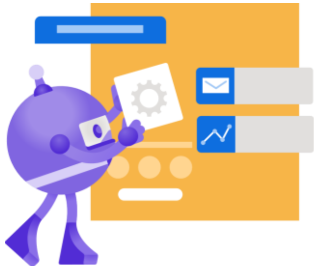
Readme | Code Beta | 0 Dependencies | 46 Dependents | 34 Versions

Microsoft Authentication Library for React (msal-react)

Install

```
> npm i @azure/msal-react
```

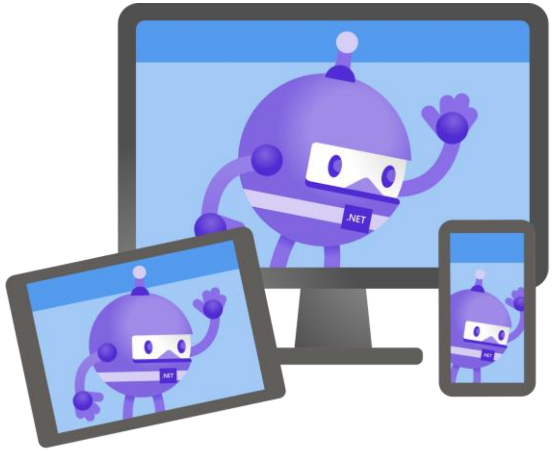
npm v1.5.1 | downloads 563k/month | codecov 95%

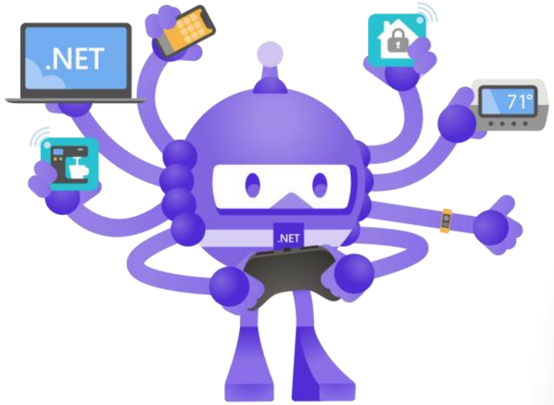


Second - authorization

1. Tenant (Company)

2. Roles



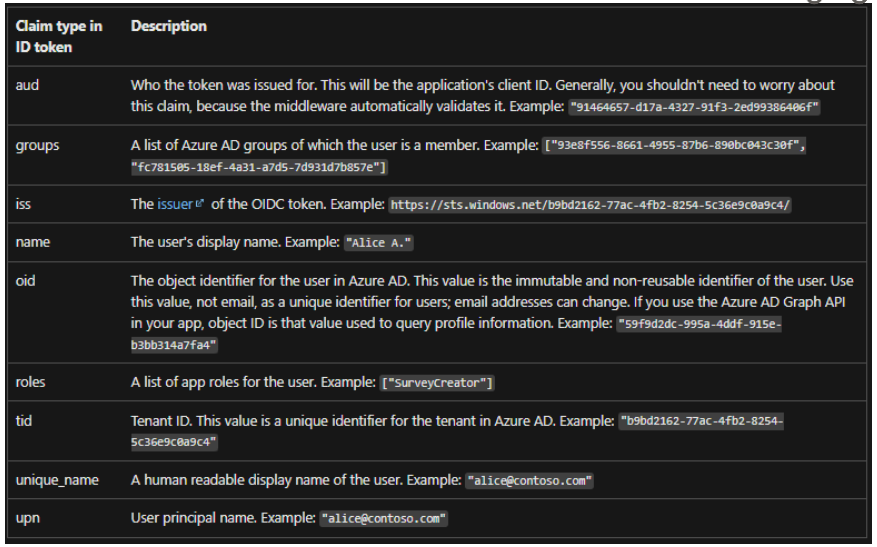


Authorization - Which Azure functionality?

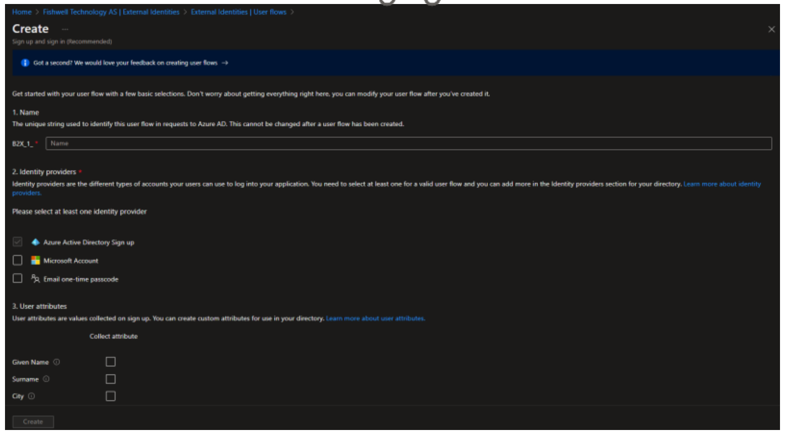
When a user signs in, Azure AD sends an ID token that contains a set of **claims** about the user. A claim is simply a piece of information, expressed as a key/value pair.

User flows are predefined, built-in, configurable policies that we provide so you can create sign-up, sign-in, and policy editing experiences in minutes.

Custom policies enable you to create your own user journeys for complex identity experience scenarios that are not supported by user flows. Azure AD B2C uses custom policies to provide extensibility.



Claim type in ID token	Description
aud	Who the token was issued for. This will be the application's client ID. Generally, you shouldn't need to worry about this claim, because the middleware automatically validates it. Example: `"91464657-d17a-4327-91f3-2ed99386406f"`
groups	A list of Azure AD groups of which the user is a member. Example: `["93e8f556-8661-4955-87b6-890bc043c30f", "fc781505-18ef-4a31-a7d5-7d931d7b857e"]`
iss	The issuer of the OIDC token. Example: `https://sts.windows.net/b9bd2162-77ac-4fb2-8254-5c36e9c0a9c4/`
name	The user's display name. Example: `"Alice A."`
oid	The object identifier for the user in Azure AD. This value is the immutable and non-reusable identifier of the user. Use this value, not email, as a unique identifier for users; email addresses can change. If you use the Azure AD Graph API in your app, object ID is that value used to query profile information. Example: `"59f9d2dc-995a-4ddf-915e-b3bb314a7fa4"`
roles	A list of app roles for the user. Example: `["SurveyCreator"]`
tid	Tenant ID. This value is a unique identifier for the tenant in Azure AD. Example: `"b9bd2162-77ac-4fb2-8254-5c36e9c0a9c4"`
unique_name	A human readable display name of the user. Example: `"alice@contoso.com"`
upn	User principal name. Example: `"alice@contoso.com"`



Home > Fishwell Technology AS | External Identities > External Identities | User flows >

Create

Sign up and sign in (Recommended)

Got a second? We would love your feedback on creating user flows →

Get started with your user flow with a few basic selections. Don't worry about getting everything right here, you can modify your user flow after you've created it.

1. Name

The unique string used to identify this user flow in requests to Azure AD. This cannot be changed after a user flow has been created.

B2X_1_ * Name

2. Identity providers *

Identity providers are the different types of accounts your users can use to log into your application. You need to select at least one for a valid user flow and you can add more in the Identity providers section for your directory. Learn more about identity providers.

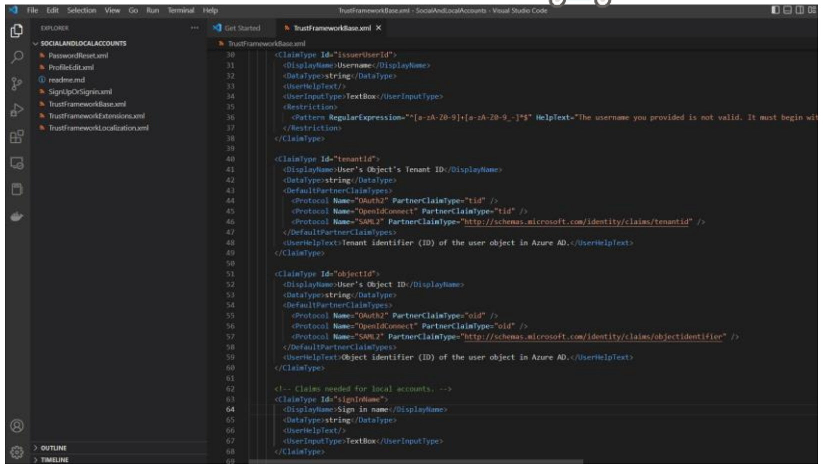
Please select at least one identity provider

☑ Azure Active Directory Sign up
□ Microsoft Account
□ Email one-time passcode

3. User attributes

User attributes are values collected on sign up. You can create custom attributes for use in your directory. Learn more about user attributes.

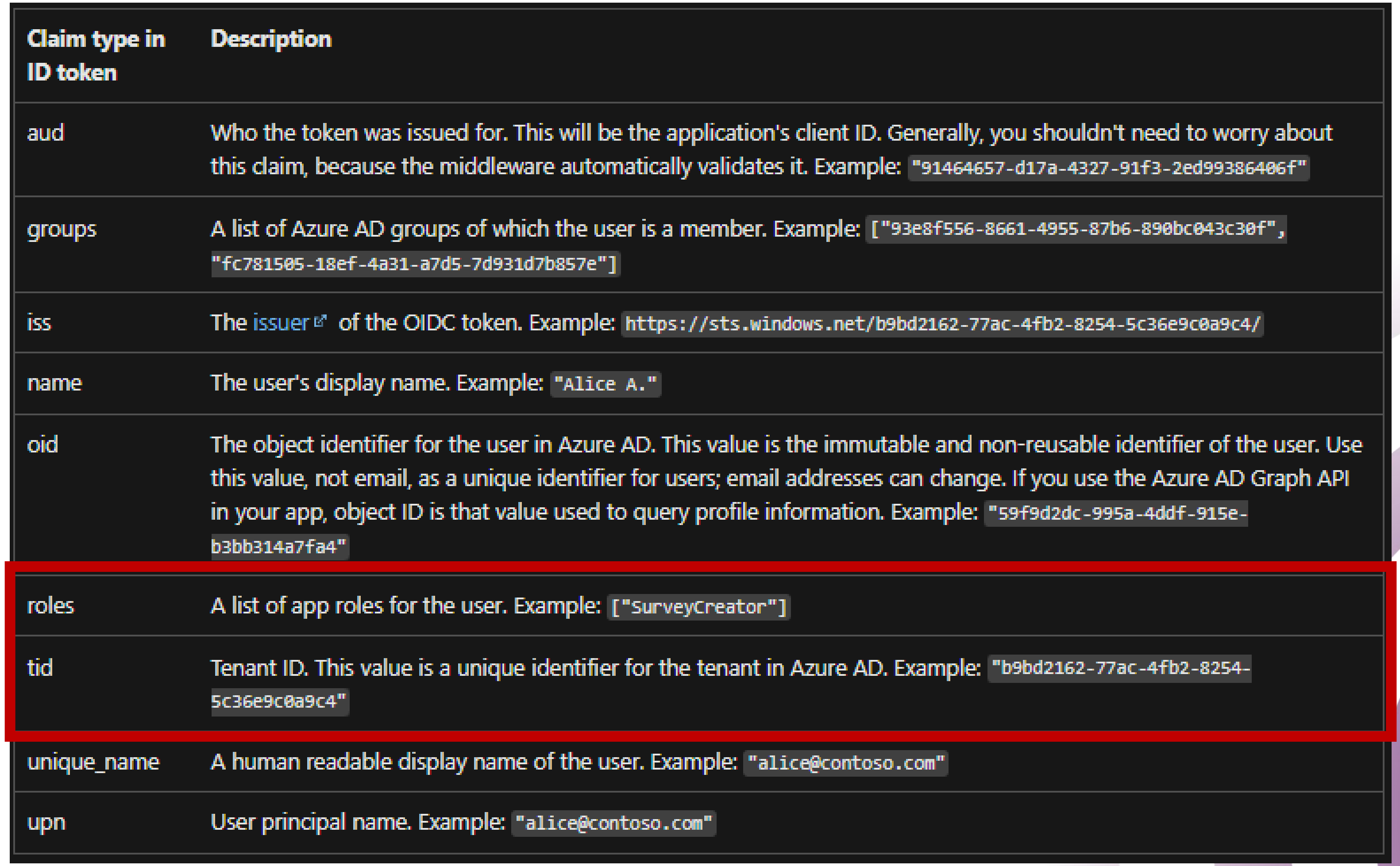
	Collect attribute
Given Name	□
Surname	□
City	□



File Edit Selection View Go Run Terminal Help
TrustFrameworkBase.xml - SocialAndLocalAccounts - Visual Studio Code
EXPLORER
SOCIALANDLOCALACCOUNTS
PasswordReset.xml
ProfileEdit.xml
readme.md
SignUpOrSignin.xml
TrustFrameworkBase.xml
TrustFrameworkExtensions.xml
TrustFrameworkLocalization.xml
Get Started
TrustFrameworkBase.xml
OUTLINE
TIMELINE

```xml
        <ClaimType Id="issuerUserId">
          <DisplayName>Username</DisplayName>
          <DataType>string</DataType>
          <UserHelpText/>
          <UserInputType>TextBox</UserInputType>
          <Restriction>
            <Pattern RegularExpression="^[a-zA-Z0-9]+[a-zA-Z0-9_-]*$" HelpText="The username you provided is not valid. It must begin wi
          </Restriction>
        </ClaimType>

        <ClaimType Id="tenantId">
          <DisplayName>User's Object's Tenant ID</DisplayName>
          <DataType>string</DataType>
          <DefaultPartnerClaimTypes>
            <Protocol Name="OAuth2" PartnerClaimType="tid" />
            <Protocol Name="OpenIdConnect" PartnerClaimType="tid" />
            <Protocol Name="SAML2" PartnerClaimType="http://schemas.microsoft.com/identity/claims/tenantid" />
          </DefaultPartnerClaimTypes>
          <UserHelpText>Tenant identifier (ID) of the user object in Azure AD.</UserHelpText>
        </ClaimType>

        <ClaimType Id="objectId">
          <DisplayName>User's Object ID</DisplayName>
          <DataType>string</DataType>
          <DefaultPartnerClaimTypes>
            <Protocol Name="OAuth2" PartnerClaimType="oid" />
            <Protocol Name="OpenIdConnect" PartnerClaimType="oid" />
            <Protocol Name="SAML2" PartnerClaimType="http://schemas.microsoft.com/identity/claims/objectidentifier" />
          </DefaultPartnerClaimTypes>
          <UserHelpText>Object identifier (ID) of the user object in Azure AD.</UserHelpText>
        </ClaimType>

        <!-- Claims needed for local accounts. -->
        <ClaimType Id="signInName">
          <DisplayName>Sign in name</DisplayName>
          <DataType>string</DataType>
          <UserHelpText/>
          <UserInputType>TextBox</UserInputType>
        </ClaimType>
```

Claims-based Identity



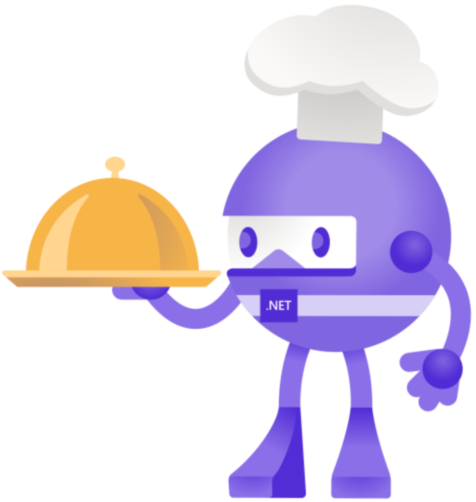
Claim type in ID token	Description
aud	Who the token was issued for. This will be the application's client ID. Generally, you shouldn't need to worry about this claim, because the middleware automatically validates it. Example: `"91464657-d17a-4327-91f3-2ed99386406f"`
groups	A list of Azure AD groups of which the user is a member. Example: `["93e8f556-8661-4955-87b6-890bc043c30f", "fc781505-18ef-4a31-a7d5-7d931d7b857e"]`
iss	The issuer of the OIDC token. Example: `https://sts.windows.net/b9bd2162-77ac-4fb2-8254-5c36e9c0a9c4/`
name	The user's display name. Example: `"Alice A."`
oid	The object identifier for the user in Azure AD. This value is the immutable and non-reusable identifier of the user. Use this value, not email, as a unique identifier for users; email addresses can change. If you use the Azure AD Graph API in your app, object ID is that value used to query profile information. Example: `"59f9d2dc-995a-4ddf-915e-b3bb314a7fa4"`
roles	A list of app roles for the user. Example: `["SurveyCreator"]`
tid	Tenant ID. This value is a unique identifier for the tenant in Azure AD. Example: `"b9bd2162-77ac-4fb2-8254-5c36e9c0a9c4"`
unique_name	A human readable display name of the user. Example: `"alice@contoso.com"`
upn	User principal name. Example: `"alice@contoso.com"`

Assign and manage roles

We define the **application roles**. After a customer signs up, an admin for the customer's AD directory assigns users to the roles. When a user signs in, the user's assigned roles are sent as claims.

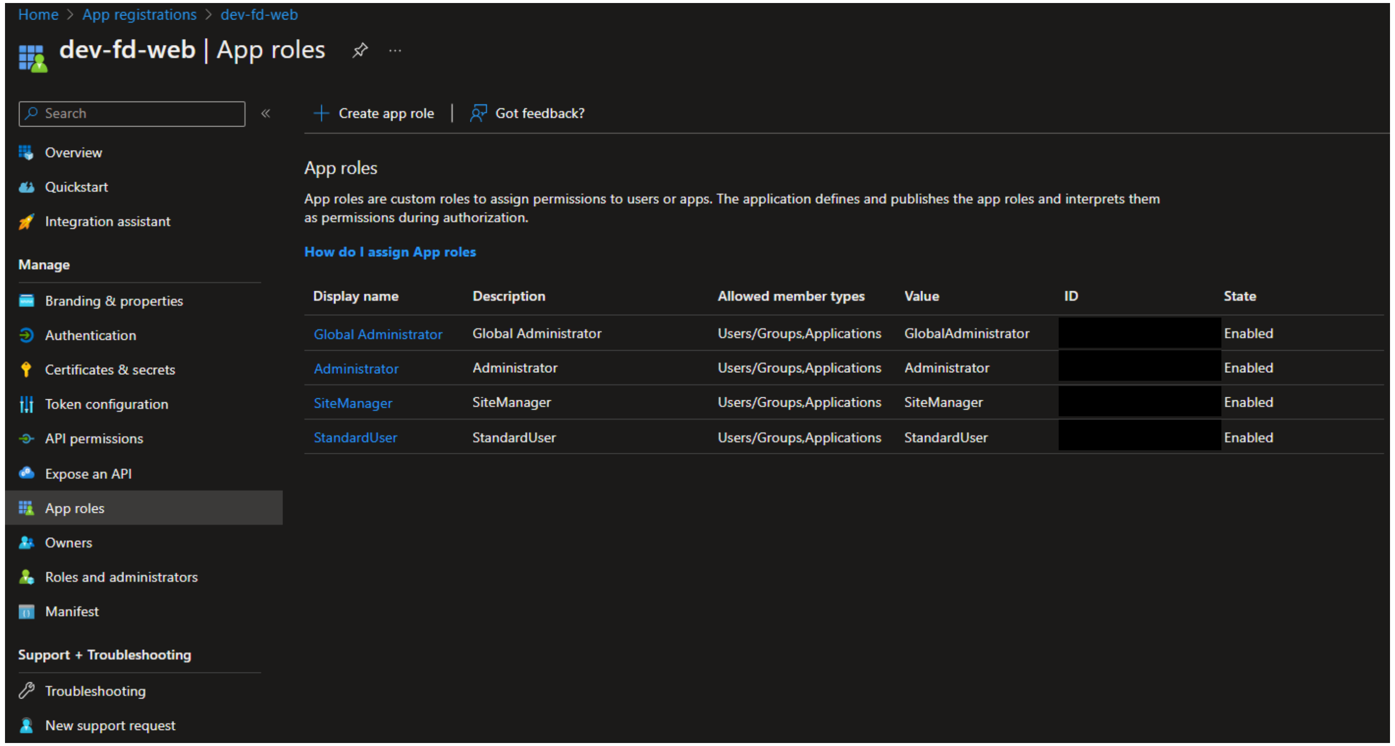
Roles are represented as Azure AD **security groups**. The application assigns permissions to users based on their security group memberships.

Application roles are not stored in Azure AD. The application stores the role assignments for each user in our own DB — for example, using the **RoleManager** class in ASP.NET Identity.



App Roles

- Global Administrator
- Administrator
- Site manager
- Standard User

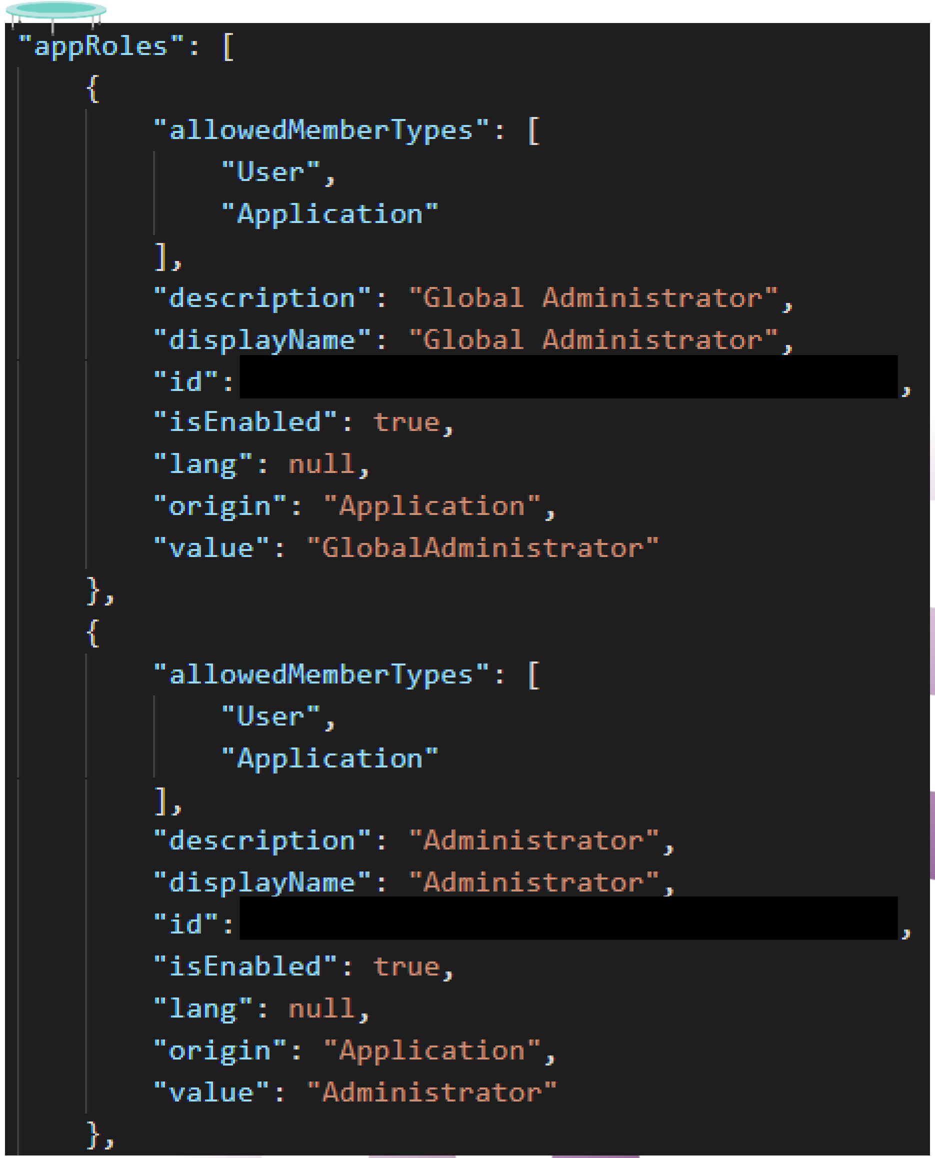


App roles

App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization.

How do I assign App roles

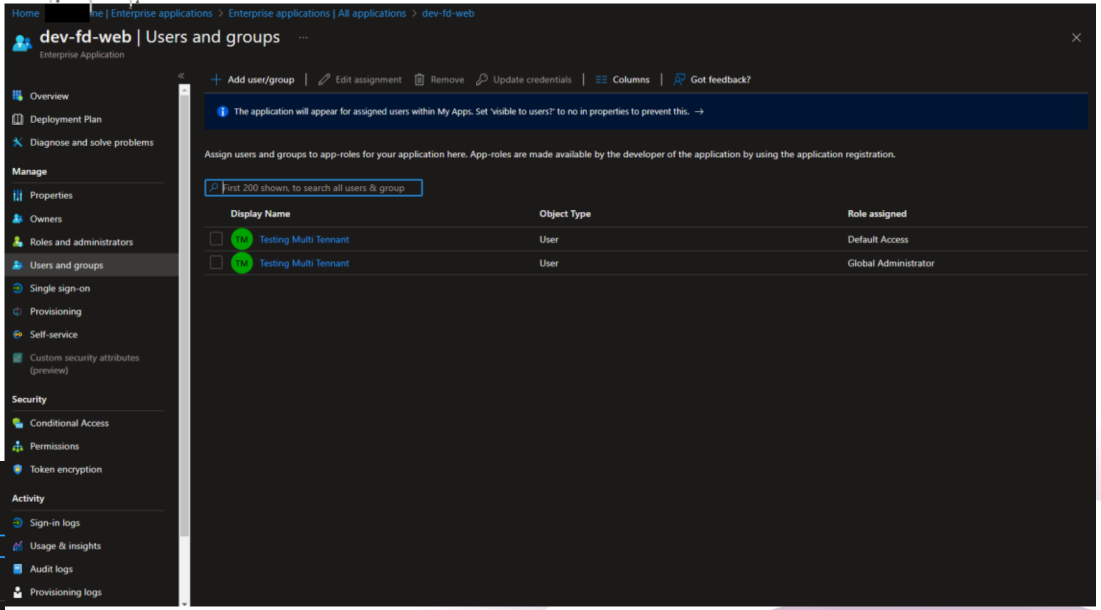
Display name	Description	Allowed member types	Value	ID	State
Global Administrator	Global Administrator	Users/Groups,Applications	GlobalAdministrator	[redacted]	Enabled
Administrator	Administrator	Users/Groups,Applications	Administrator	[redacted]	Enabled
SiteManager	SiteManager	Users/Groups,Applications	SiteManager	[redacted]	Enabled
StandardUser	StandardUser	Users/Groups,Applications	StandardUser	[redacted]	Enabled



```
"appRoles": [
    {
        "allowedMemberTypes": [
            "User",
            "Application"
        ],
        "description": "Global Administrator",
        "displayName": "Global Administrator",
        "id": [redacted],
        "isEnabled": true,
        "lang": null,
        "origin": "Application",
        "value": "GlobalAdministrator"
    },
    {
        "allowedMemberTypes": [
            "User",
            "Application"
        ],
        "description": "Administrator",
        "displayName": "Administrator",
        "id": [redacted],
        "isEnabled": true,
        "lang": null,
        "origin": "Application",
        "value": "Administrator"
    },
```

App Roles

- Global Administrator
- Administrator
- Site manager
- Standard User



Home [redacted] ne | Enterprise applications > Enterprise applications | All applications > dev-fd-web

dev-fd-web | Users and groups

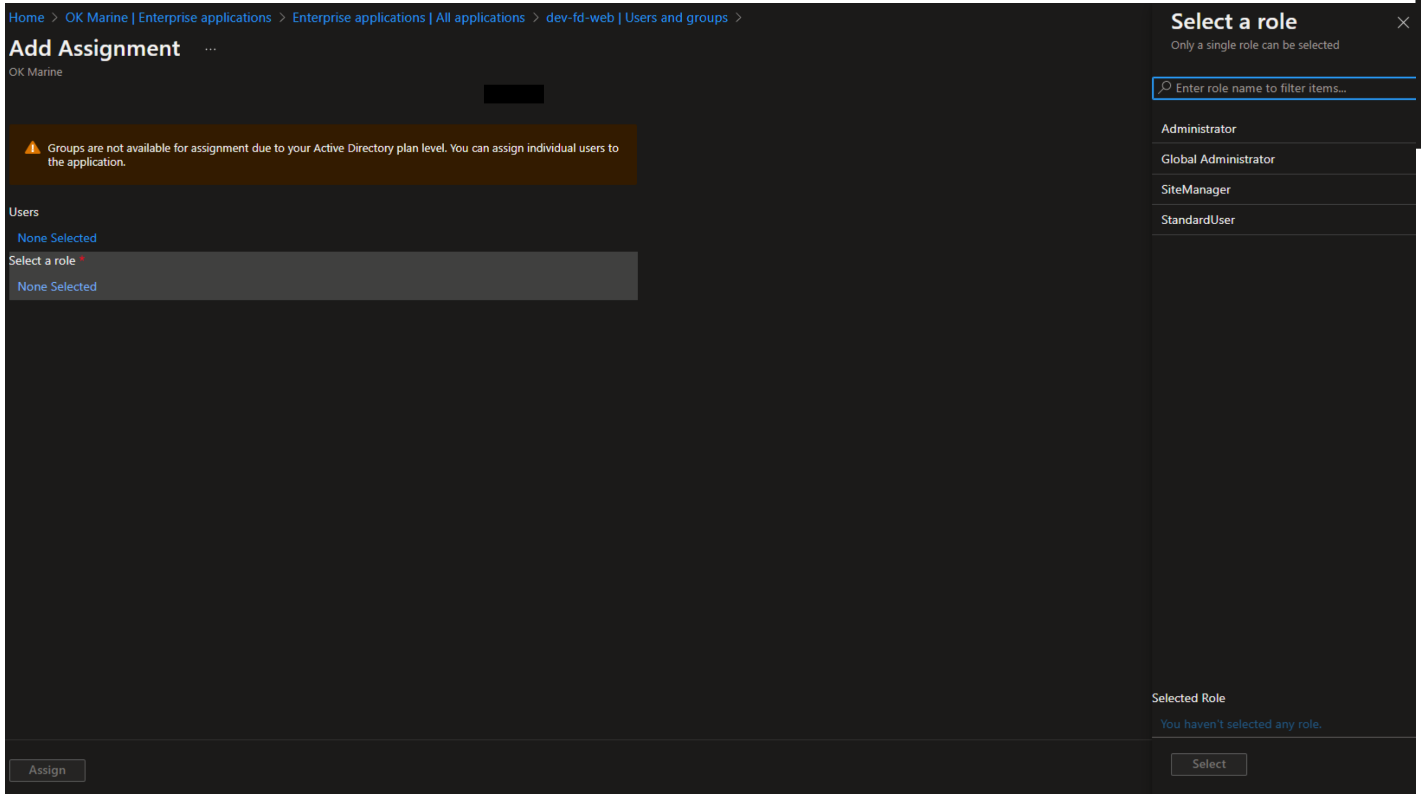
Enterprise Application

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

Assign users and groups to app-roles for your application here. App-roles are made available by the developer of the application by using the application registration.

First 200 shown, to search all users & group

	Display Name	Object Type	Role assigned
□	TM Testing Multi Tennant	User	Default Access
□	TM Testing Multi Tennant	User	Global Administrator



Home > OK Marine | Enterprise applications > Enterprise applications | All applications > dev-fd-web | Users and groups >

Add Assignment

OK Marine

[redacted]

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

None Selected

Select a role *

None Selected

Select a role

Only a single role can be selected

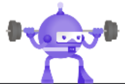
Enter role name to filter items...

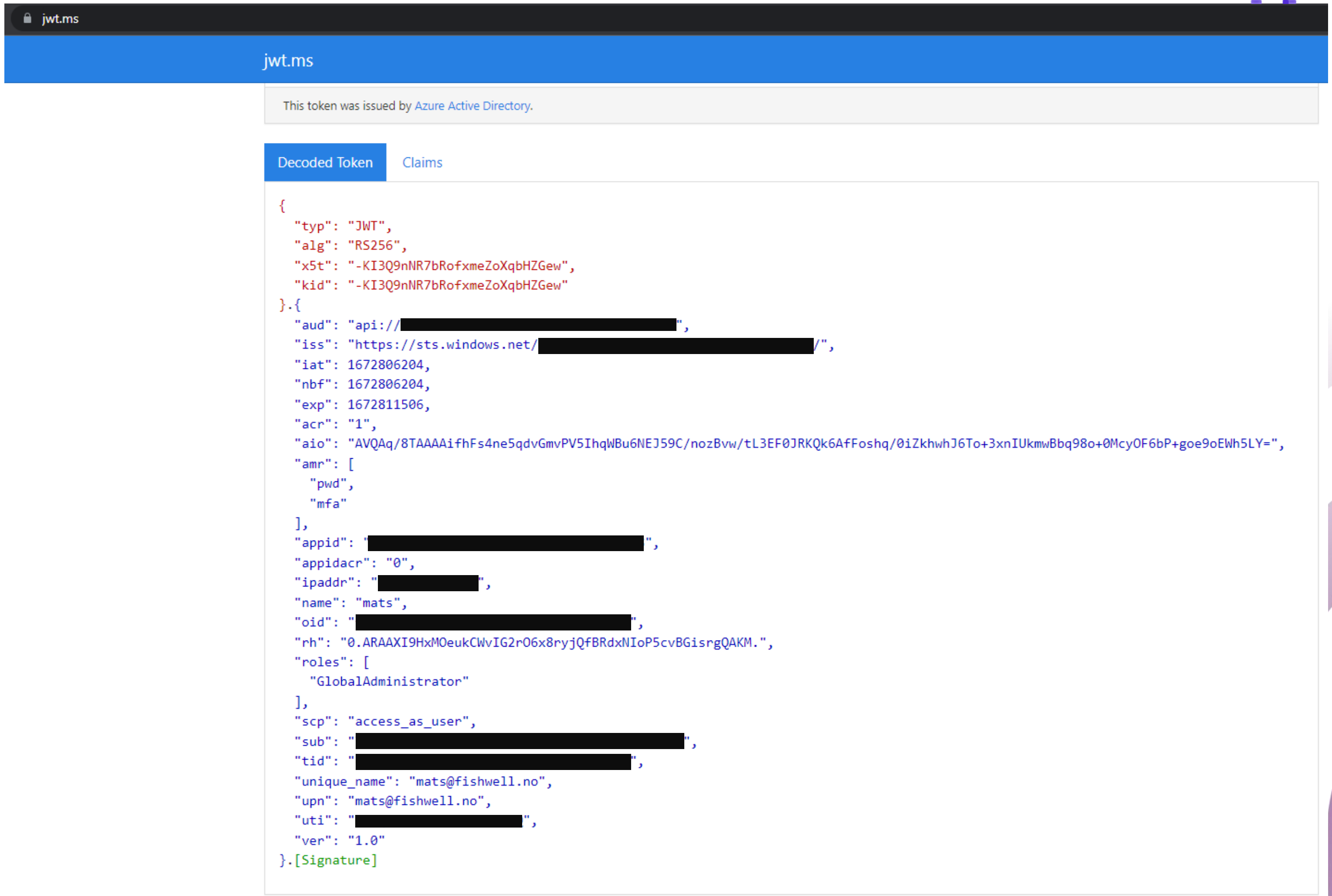
- Administrator
- Global Administrator
- SiteManager
- StandardUser

Selected Role

You haven't selected any role.

JWT Example





jwt.ms

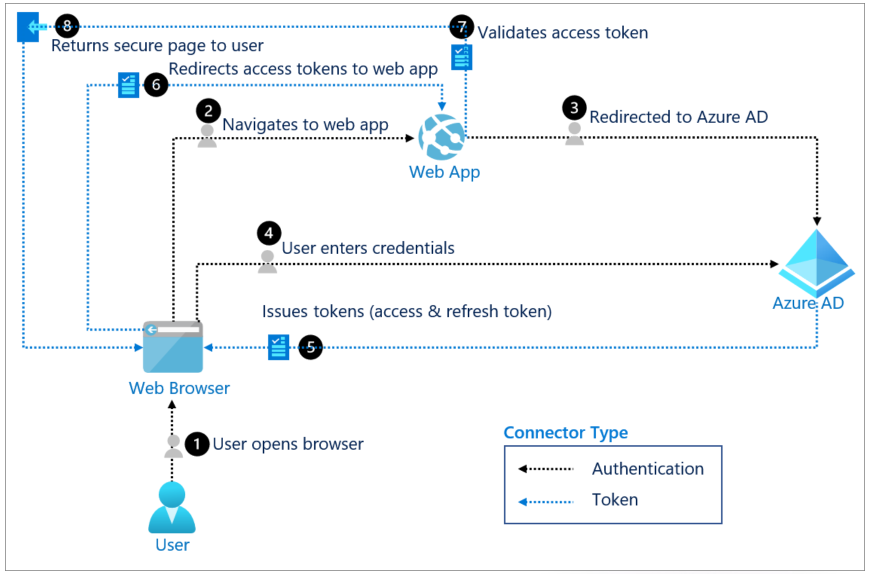
jwt.ms

This token was issued by Azure Active Directory.

Decoded Token | Claims

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "-KI3Q9nNR7bRofxmeZoXqbHZGew",
  "kid": "-KI3Q9nNR7bRofxmeZoXqbHZGew"
}.{
  "aud": "api://[redacted]",
  "iss": "https://sts.windows.net/[redacted]/",
  "iat": 1672806204,
  "nbf": 1672806204,
  "exp": 1672811506,
  "acr": "1",
  "aio": "AVQAq/8TAAAAifhFs4ne5qdvGmvPV5IhqWBu6NEJ59C/nozBvw/tL3EF0JRKQk6AfFoshq/0iZkhwhJ6To+3xnIUkmwBbq98o+0McyOF6bP+goe9oEWh5LY=",
  "amr": [
    "pwd",
    "mfa"
  ],
  "appid": "[redacted]",
  "appidacr": "0",
  "ipaddr": "[redacted]",
  "name": "mats",
  "oid": "[redacted]",
  "rh": "0.ARAAXI9HxMOeukCWvIG2rO6x8ryjQfBRdxNIoP5cvBGisrgQAKM.",
  "roles": [
    "GlobalAdministrator"
  ],
  "scp": "access_as_user",
  "sub": "[redacted]",
  "tid": "[redacted]",
  "unique_name": "mats@fishwell.no",
  "upn": "mats@fishwell.no",
  "uti": "[redacted]",
  "ver": "1.0"
}.[Signature]
```

OAuth 2.0 and OpenID Connect (OIDC)



OAuth 2.0

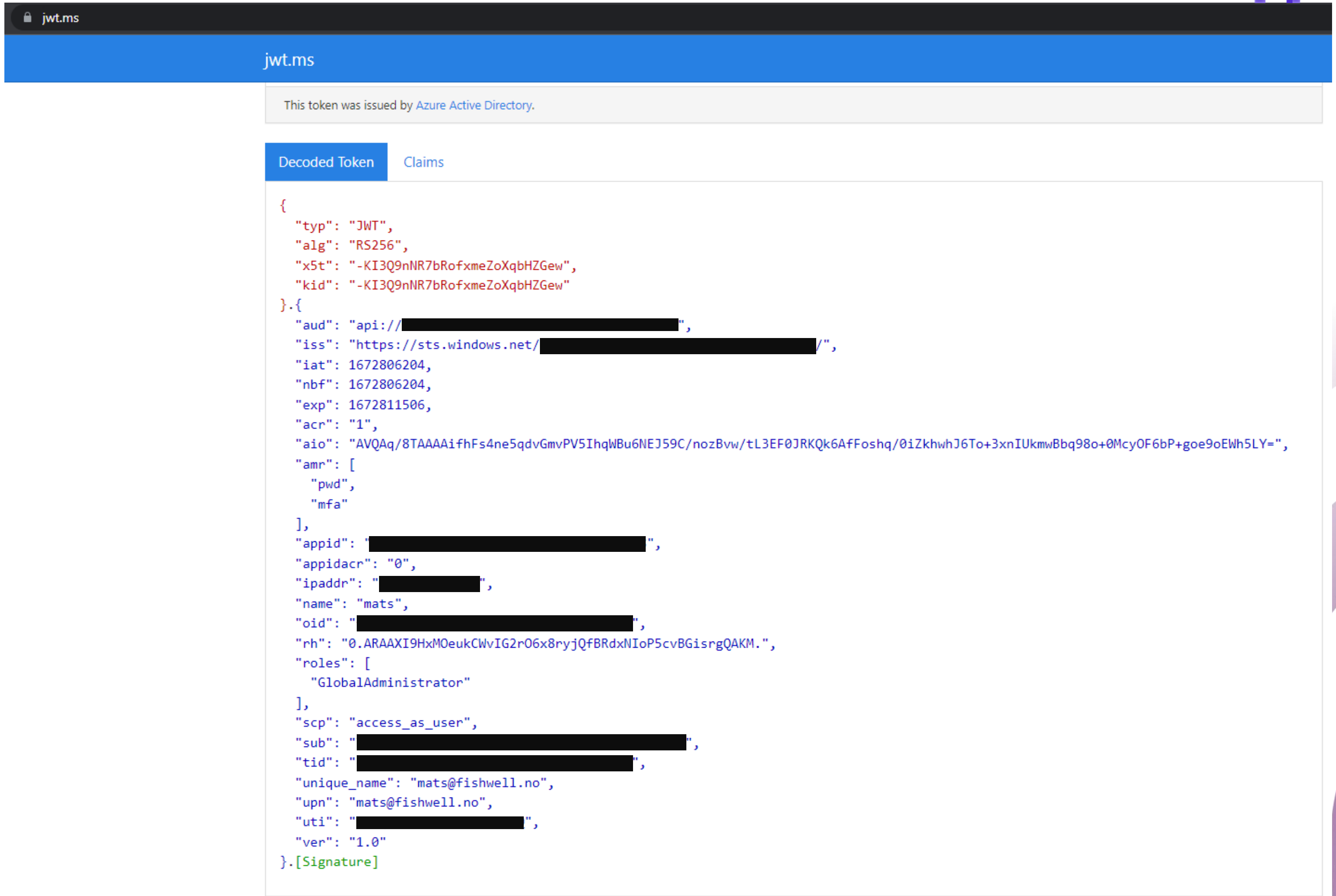
ACCESS TOKEN

OpenID Connect

ID TOKEN

https://openid.net/specs/openid-connect-core-1_0.html

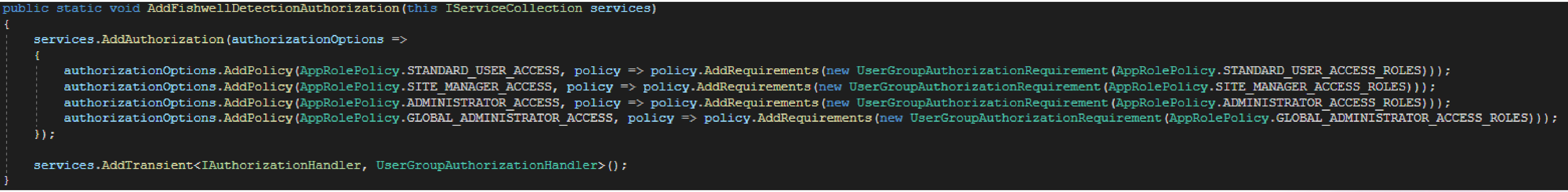
JWT Example



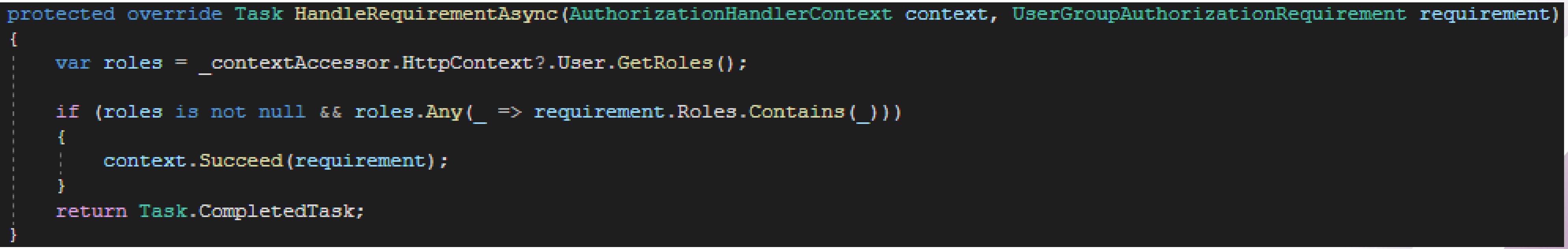
This token was issued by Azure Active Directory.

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "-KI3Q9nNR7bRofxmeZoXqbHZGew",
  "kid": "-KI3Q9nNR7bRofxmeZoXqbHZGew"
}.{
  "aud": "api://[redacted]",
  "iss": "https://sts.windows.net/[redacted]/",
  "iat": 1672806204,
  "nbf": 1672806204,
  "exp": 1672811506,
  "acr": "1",
  "aio": "AVQAq/8TAAAAifhFs4ne5qdvGmvPV5IhqWBu6NEJ59C/nozBvw/tL3EF0JRKQk6AfFoshq/0iZkhwhJ6To+3xnIUkmwBbq98o+0McyOF6bP+goe9oEWh5LY=",
  "amr": [
    "pwd",
    "mfa"
  ],
  "appid": "[redacted]",
  "appidacr": "0",
  "ipaddr": "[redacted]",
  "name": "mats",
  "oid": "[redacted]",
  "rh": "0.ARAAXI9HxMOeukCWvIG2rO6x8ryjQfBRdxNIoP5cvBGisrgQAKM.",
  "roles": [
    "GlobalAdministrator"
  ],
  "scp": "access_as_user",
  "sub": "[redacted]",
  "tid": "[redacted]",
  "unique_name": "mats@fishwell.no",
  "upn": "mats@fishwell.no",
  "uti": "[redacted]",
  "ver": "1.0"
}.[Signature]
```

Using the information from the claim

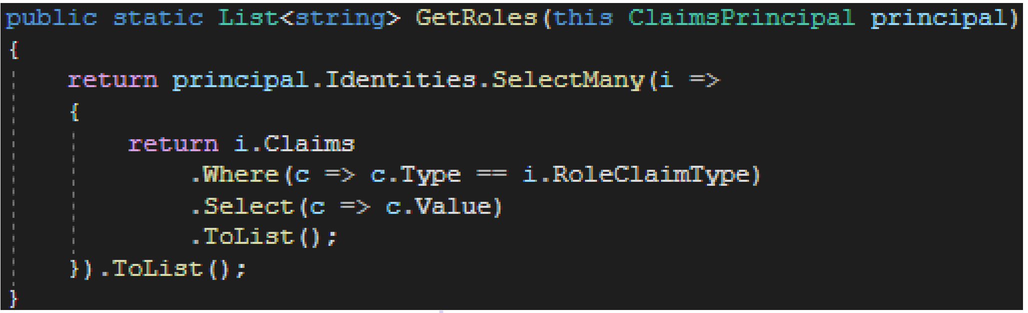


```
public static void AddFishwellDetectionAuthorization(this IServiceCollection services)
{
    services.AddAuthorization(authorizationOptions =>
    {
        authorizationOptions.AddPolicy(AppRolePolicy.STANDARD_USER_ACCESS, policy => policy.AddRequirements(new UserGroupAuthorizationRequirement(AppRolePolicy.STANDARD_USER_ACCESS_ROLES)));
        authorizationOptions.AddPolicy(AppRolePolicy.SITE_MANAGER_ACCESS, policy => policy.AddRequirements(new UserGroupAuthorizationRequirement(AppRolePolicy.SITE_MANAGER_ACCESS_ROLES)));
        authorizationOptions.AddPolicy(AppRolePolicy.ADMINISTRATOR_ACCESS, policy => policy.AddRequirements(new UserGroupAuthorizationRequirement(AppRolePolicy.ADMINISTRATOR_ACCESS_ROLES)));
        authorizationOptions.AddPolicy(AppRolePolicy.GLOBAL_ADMINISTRATOR_ACCESS, policy => policy.AddRequirements(new UserGroupAuthorizationRequirement(AppRolePolicy.GLOBAL_ADMINISTRATOR_ACCESS_ROLES)));
    });

    services.AddTransient<IAuthorizationHandler, UserGroupAuthorizationHandler>();
}
```

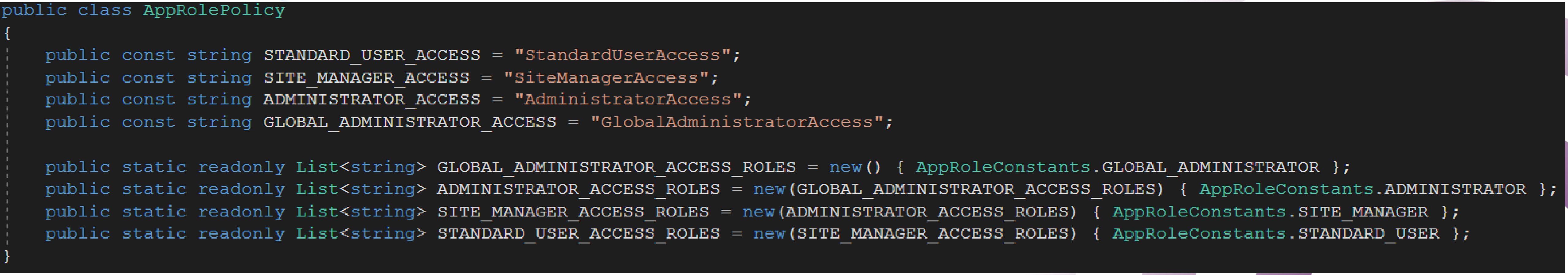


```
protected override Task HandleRequirementAsync(AuthorizationHandlerContext context, UserGroupAuthorizationRequirement requirement)
{
    var roles = _contextAccessor.HttpContext?.User.GetRoles();

    if (roles is not null && roles.Any(_ => requirement.Roles.Contains(_)))
    {
        context.Succeed(requirement);
    }
    return Task.CompletedTask;
}
```

Using the information from the claim

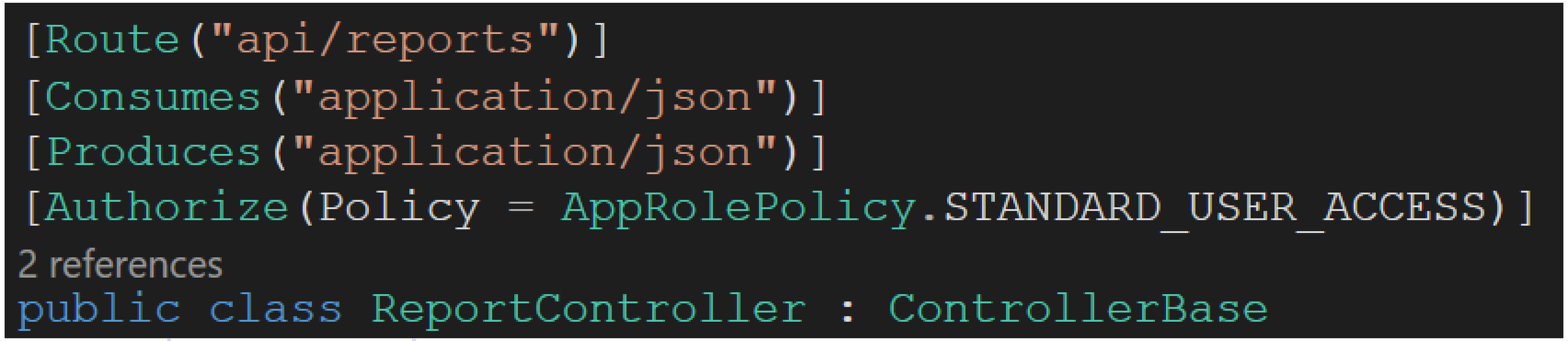


```
public static List<string> GetRoles(this ClaimsPrincipal principal)
{
    return principal.Identities.SelectMany(i =>
    {
        return i.Claims
            .Where(c => c.Type == i.RoleClaimType)
            .Select(c => c.Value)
            .ToList();
    }).ToList();
}
```

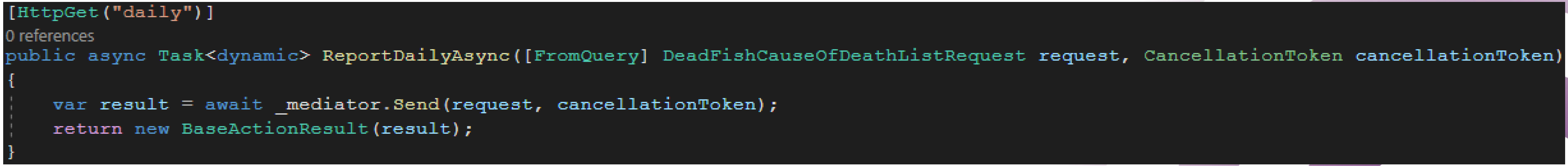


```
public class AppRolePolicy
{
    public const string STANDARD_USER_ACCESS = "StandardUserAccess";
    public const string SITE_MANAGER_ACCESS = "SiteManagerAccess";
    public const string ADMINISTRATOR_ACCESS = "AdministratorAccess";
    public const string GLOBAL_ADMINISTRATOR_ACCESS = "GlobalAdministratorAccess";

    public static readonly List<string> GLOBAL_ADMINISTRATOR_ACCESS_ROLES = new() { AppRoleConstants.GLOBAL_ADMINISTRATOR };
    public static readonly List<string> ADMINISTRATOR_ACCESS_ROLES = new(GLOBAL_ADMINISTRATOR_ACCESS_ROLES) { AppRoleConstants.ADMINISTRATOR };
    public static readonly List<string> SITE_MANAGER_ACCESS_ROLES = new(ADMINISTRATOR_ACCESS_ROLES) { AppRoleConstants.SITE_MANAGER };
    public static readonly List<string> STANDARD_USER_ACCESS_ROLES = new(SITE_MANAGER_ACCESS_ROLES) { AppRoleConstants.STANDARD_USER };
}
```

Using the information from the claim

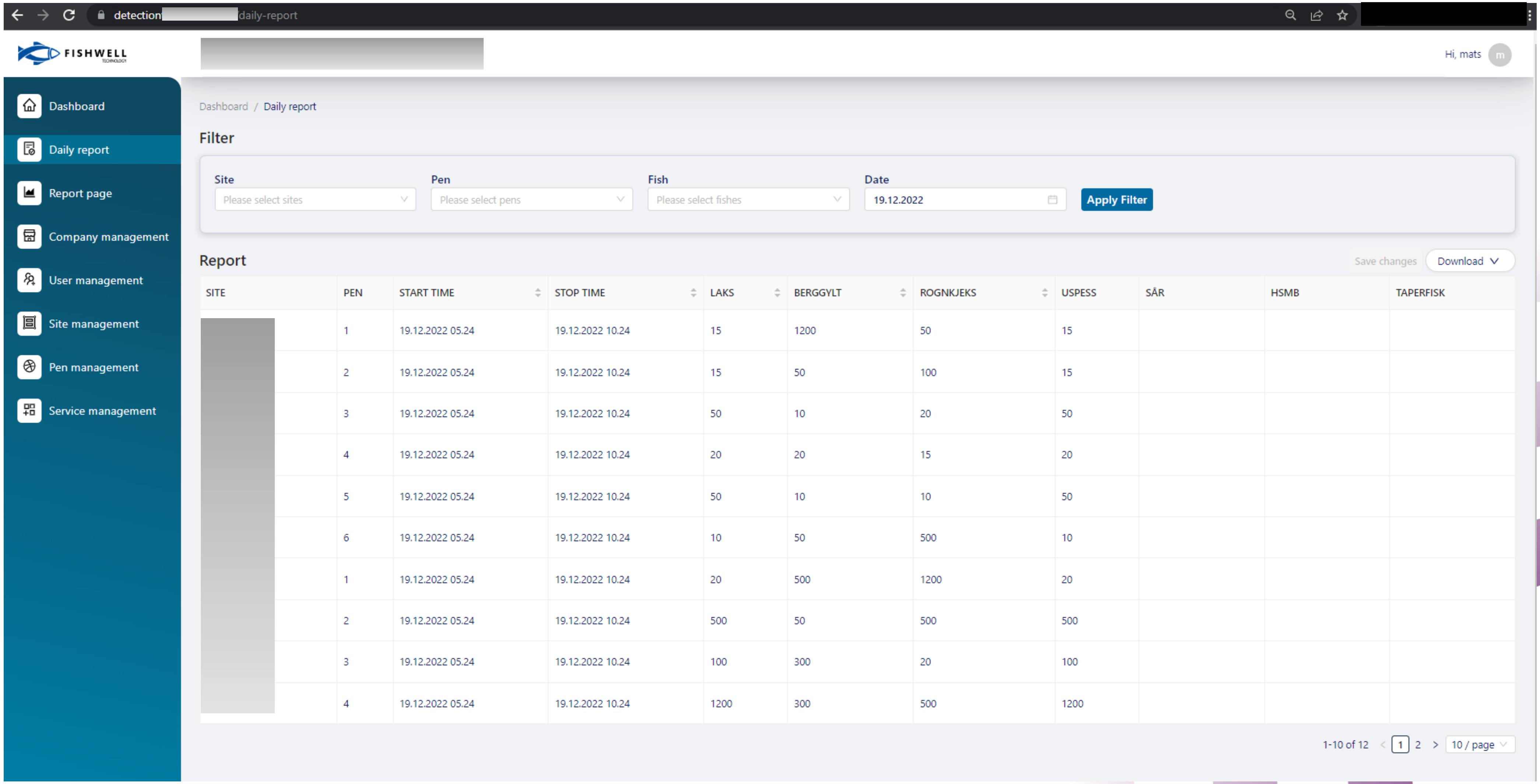


```
[Route("api/reports")]
[Consumes("application/json")]
[Produces("application/json")]
[Authorize(Policy = AppRolePolicy.STANDARD_USER_ACCESS)]
2 references
public class ReportController : ControllerBase
```



```
[HttpGet("daily")]
0 references
public async Task<dynamic> ReportDailyAsync([FromQuery] DeadFishCauseOfDeathListRequest request, CancellationToken cancellationToken)
{
    var result = await _mediator.Send(request, cancellationToken);
    return new BaseActionResult(result);
}
```

Our dead fish counter - Fishwell Detection



detection[redacted]daily-report [redacted]

FISHWELL TECHNOLOGY [redacted]

Hi, mats m

Dashboard / Daily report

Filter

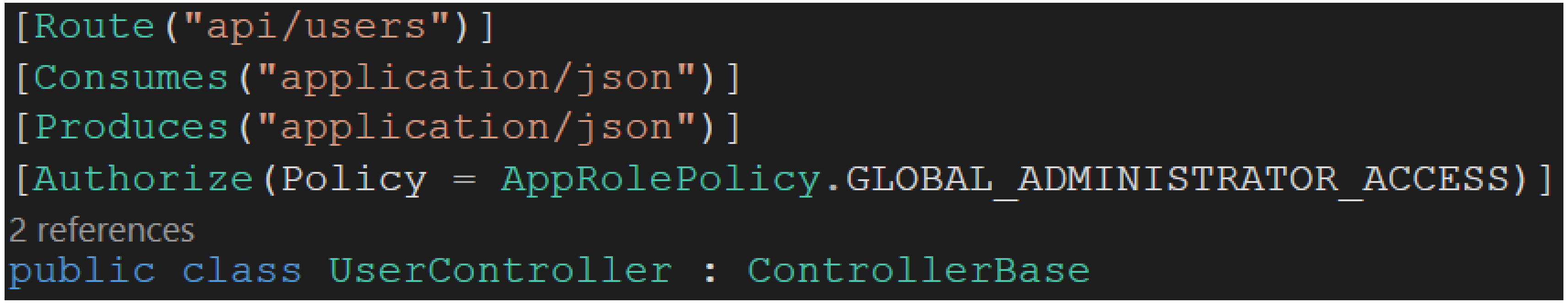
Site: Please select sites
Pen: Please select pens
Fish: Please select fishes
Date: 19.12.2022

Report

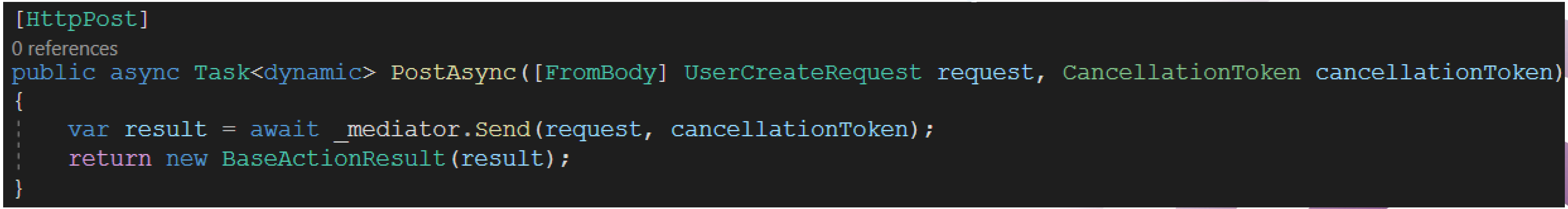
SITE	PEN	START TIME	STOP TIME	LAKS	BERGGYLT	ROGNKJEKS	USPESS	SÅR	HSMB	TAPERFISK
[redacted]	1	19.12.2022 05.24	19.12.2022 10.24	15	1200	50	15			
[redacted]	2	19.12.2022 05.24	19.12.2022 10.24	15	50	100	15			
[redacted]	3	19.12.2022 05.24	19.12.2022 10.24	50	10	20	50			
[redacted]	4	19.12.2022 05.24	19.12.2022 10.24	20	20	15	20			
[redacted]	5	19.12.2022 05.24	19.12.2022 10.24	50	10	10	50			
[redacted]	6	19.12.2022 05.24	19.12.2022 10.24	10	50	500	10			
[redacted]	1	19.12.2022 05.24	19.12.2022 10.24	20	500	1200	20			
[redacted]	2	19.12.2022 05.24	19.12.2022 10.24	500	50	500	500			
[redacted]	3	19.12.2022 05.24	19.12.2022 10.24	100	300	20	100			
[redacted]	4	19.12.2022 05.24	19.12.2022 10.24	1200	300	500	1200			

1-10 of 12 < 1 2 > 10 / page

Using the information from the claim

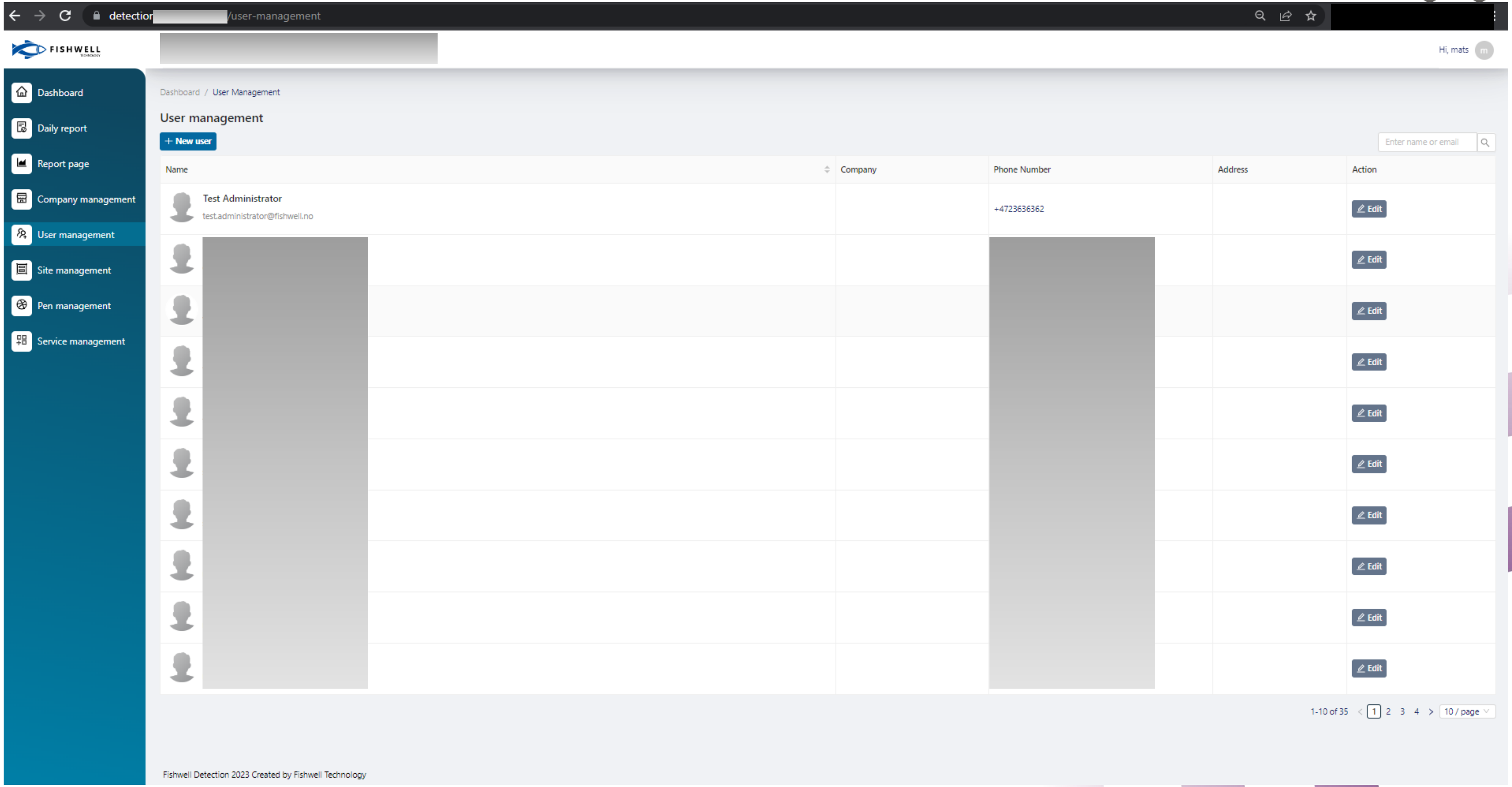


```
[Route("api/users")]
[Consumes("application/json")]
[Produces("application/json")]
[Authorize(Policy = AppRolePolicy.GLOBAL_ADMINISTRATOR_ACCESS)]
2 references
public class UserController : ControllerBase
```



```
[HttpPost]
0 references
public async Task<dynamic> PostAsync([FromBody] UserCreateRequest request, CancellationToken cancellationToken)
{
    var result = await _mediator.Send(request, cancellationToken);
    return new BaseActionResult(result);
}
```

Our dead fish counter - Fishwell Detection



Dashboard / User Management

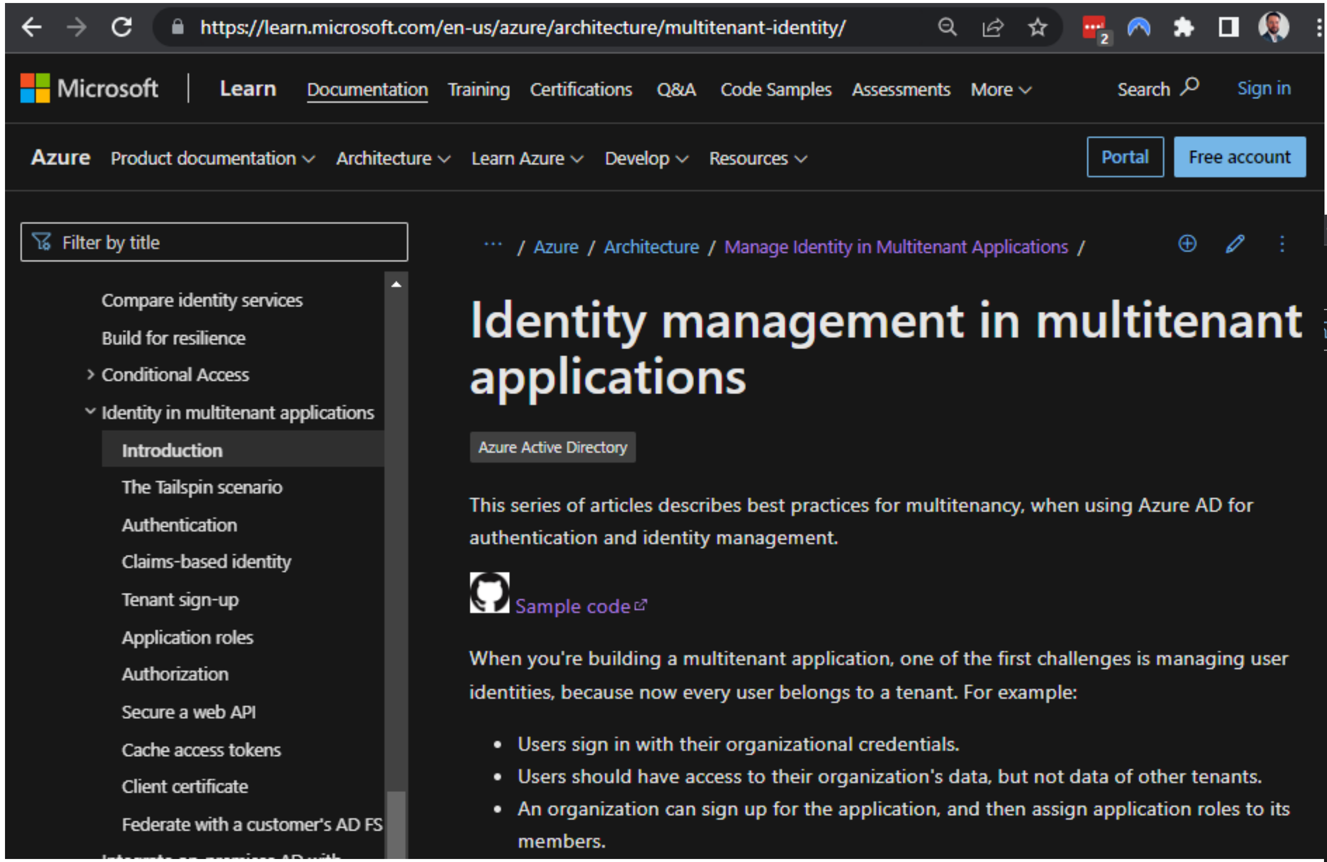
User management

Name	Company	Phone Number	Address	Action
Test Administrator test.administrator@fishwell.no		+4723636362		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit
[redacted]		[redacted]		Edit

Fishwell Detection 2023 Created by Fishwell Technology

Look more into how to set this up

https://learn.microsoft.com/en-us/azure/architecture/multitenant-identity/



Identity management in multitenant applications

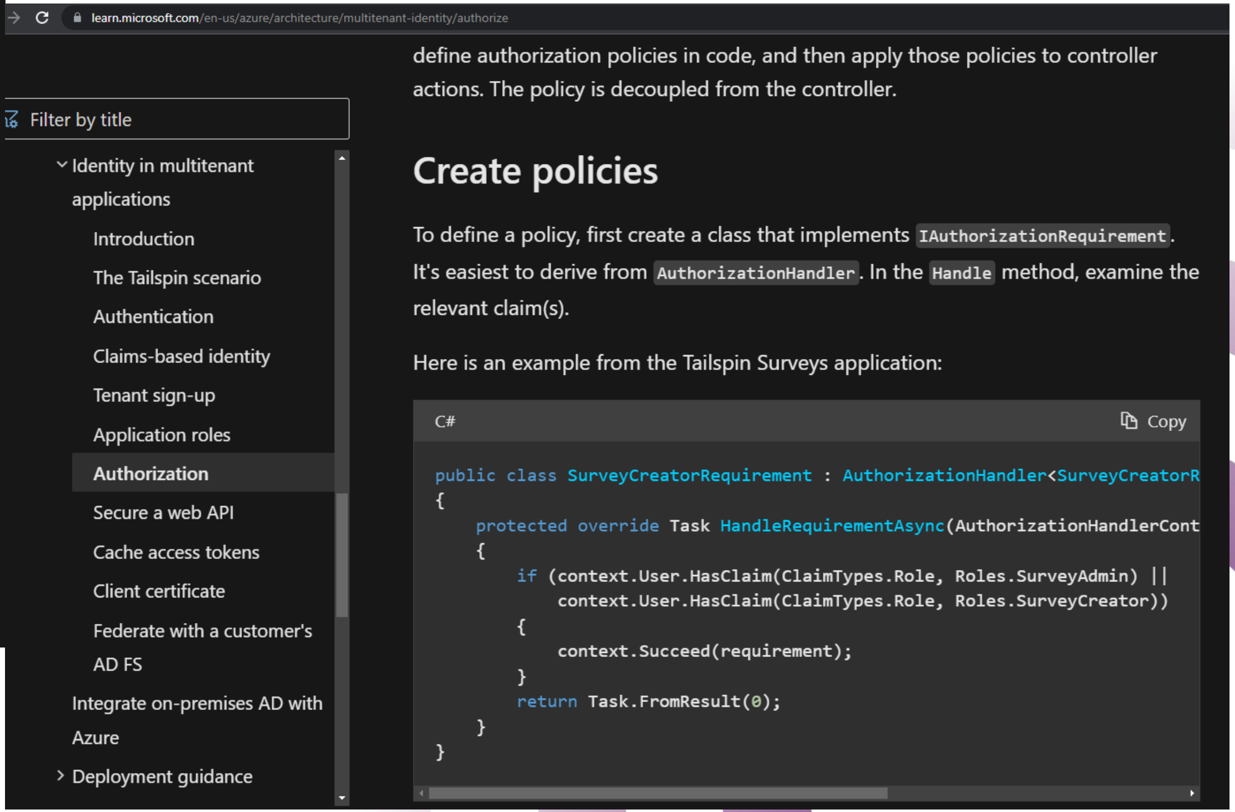
Azure Active Directory

This series of articles describes best practices for multitenancy, when using Azure AD for authentication and identity management.

Sample code

When you're building a multitenant application, one of the first challenges is managing user identities, because now every user belongs to a tenant. For example:

- Users sign in with their organizational credentials.
- Users should have access to their organization's data, but not data of other tenants.
- An organization can sign up for the application, and then assign application roles to its members.



define authorization policies in code, and then apply those policies to controller actions. The policy is decoupled from the controller.

Create policies

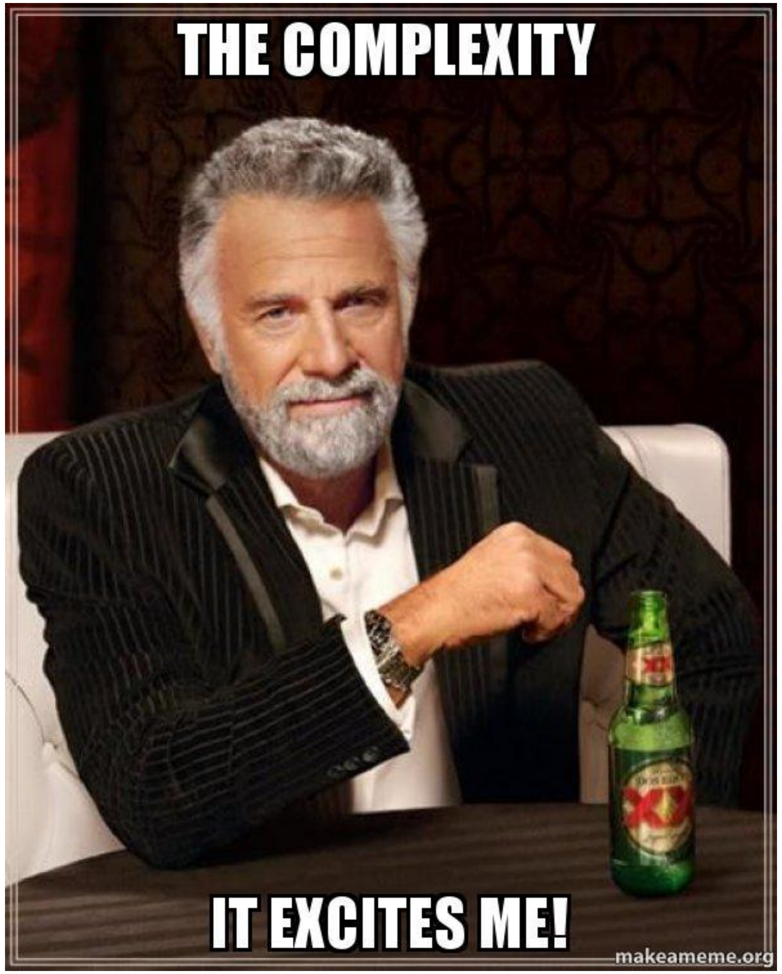
To define a policy, first create a class that implements `IAuthorizationRequirement`. It's easiest to derive from `AuthorizationHandler`. In the `Handle` method, examine the relevant claim(s).

Here is an example from the Tailspin Surveys application:

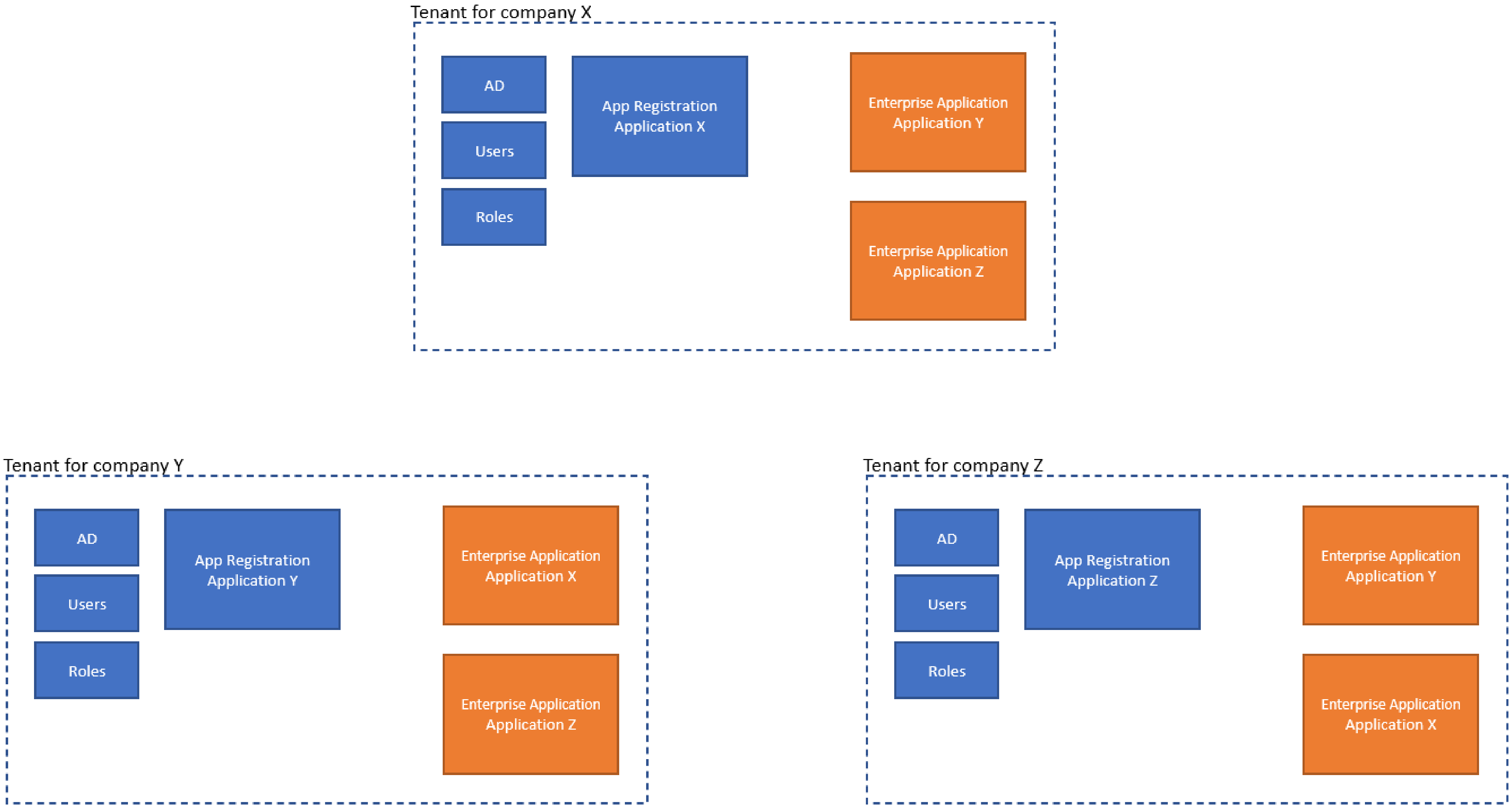
C# Copy

```
public class SurveyCreatorRequirement : AuthorizationHandler<SurveyCreatorR
{
    protected override Task HandleRequirementAsync(AuthorizationHandlerCont
    {
        if (context.User.HasClaim(ClaimTypes.Role, Roles.SurveyAdmin) ||
            context.User.HasClaim(ClaimTypes.Role, Roles.SurveyCreator))
        {
            context.Succeed(requirement);
        }
        return Task.FromResult(0);
    }
}
```

Creating an ecosystem of applications



Creating an ecosystem of applications



Tenant for company X

AD

Users

Roles

App Registration Application X

Enterprise Application Application Y

Enterprise Application Application Z

Tenant for company Y

AD

Users

Roles

App Registration Application Y

Enterprise Application Application X

Enterprise Application Application Z

Tenant for company Z

AD

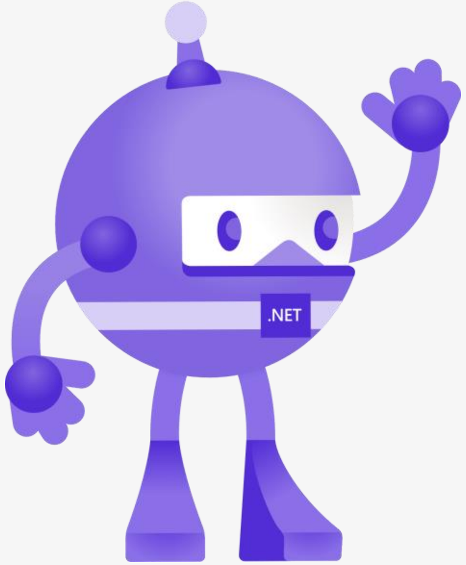
Users

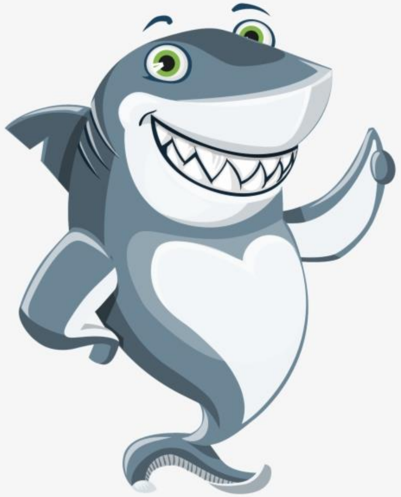
Roles

App Registration Application Z

Enterprise Application Application Y

Enterprise Application Application X





Any questions?

Email: mats@fishwell.no

LinkedIn: https://www.linkedin.com/in/matslundellnygjelten/

Thank you!

Email: mats@fishwell.no

LinkedIn: https://www.linkedin.com/in/matslundellnygjelten/