Single Sign-on & User Provisioning

Versie	1.0
Datum	15-12-2023

Easy Systems BV
Oortlaan 2
6716 WD EDE
T +31 (0)318 648 748
E info@easysystems.nl

Single Sign-On & User Provisioning with Microsoft Entra ID
Information about Single Sign-On & User Provisioning regarding Easy Systems applications

1 Introduction

This document describes the Single Sign-On and User-Provisioning functionality regarding Easy Systems application Easy Invoice.

Requirements:

- Identity Provider based on OAuth.
- Microsoft Entra ID for user-provisioning

User Provisioning is the process of importing users in your application. The importing of users is done via the Microsoft Graph API.

With Single Sign-On it is possible to use an external Identity Provider to login to the Easy Systems applications.

The customer needs to provide the following requirements before Easy Invoice can integrate with Entra ID.

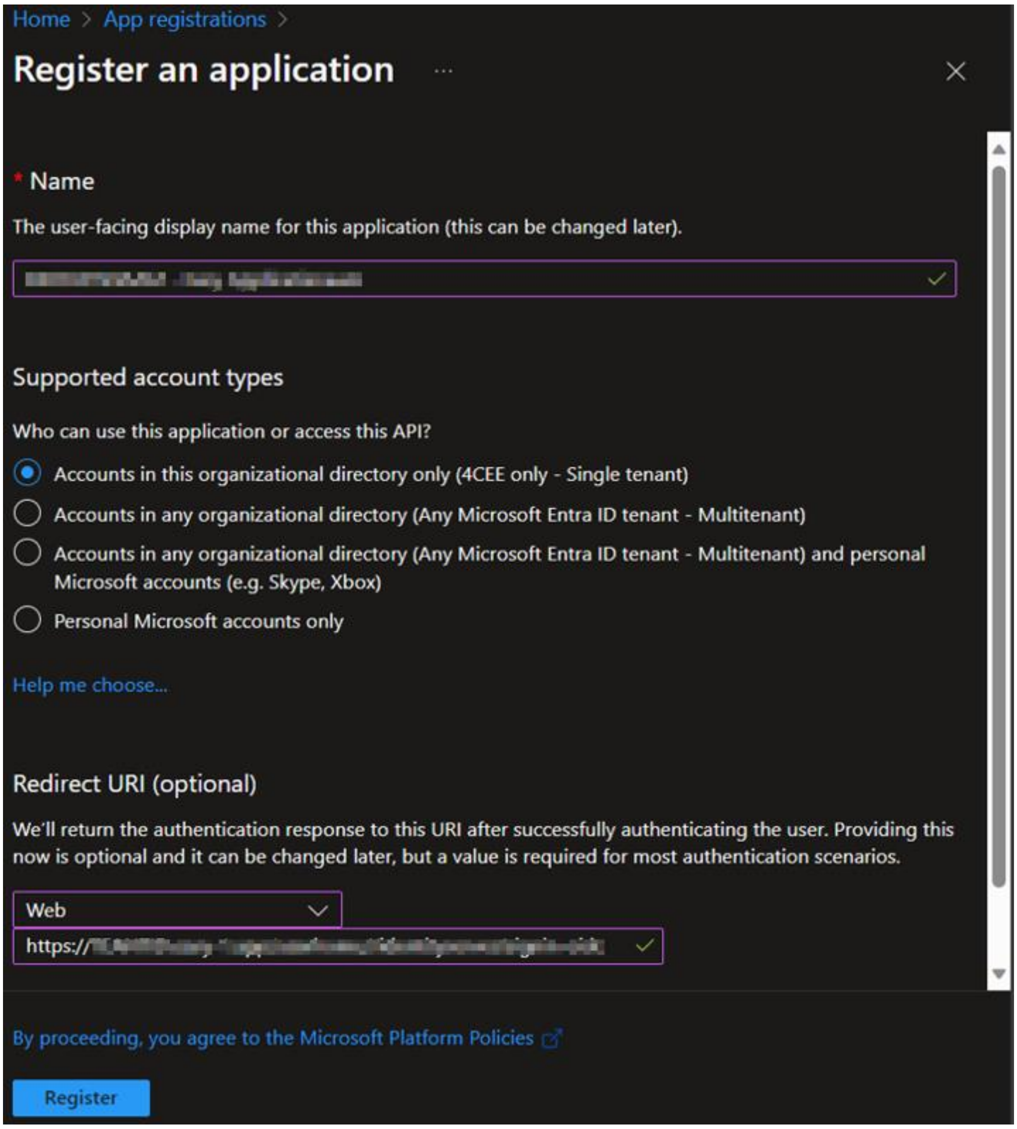
- One app registration with the described requirements for Single Sign-On and User Provisioning.
    - Tenant ID
    - Client ID
    - Client Secret
    - Active Directory Easy Systems User credentials
        - Username
        - Password

2 Microsoft Entra ID

Log in to the Entra Portal. You can do this via https://entra.microsoft.com. Click on ‘Applications’ in the left column and select ‘App Registrations’.

2.1 Register an application

Create a new App registration and enter the Easy Invoice URL in the Redirect URI. This is often https://customername.easysystems.app/easyinvoice/ and will be supplied by the Easy Systems consultant. Please note, the last slash in the URL is required for Easy Invoice to function correctly.



* Name

The user-facing display name for this application (this can be changed later).

[redacted] ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (4CEE only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

https://[redacted] ✓

Figure 1: Register an application

Now open the application you just created and complete the following steps.

2.2 Authentication

Select Authentication in the left menu and make sure that 'ID Tokens' (used for implicit and hybrid flows) is checked, save this.

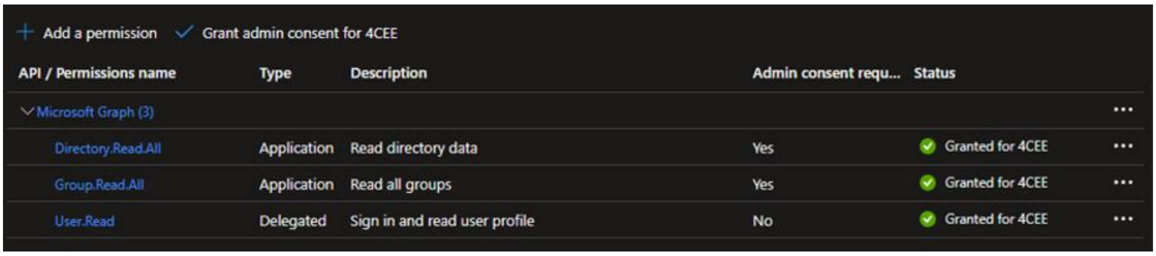
If the customer has forgotten to enter the redirect URI when creating the app registration, this must be done here.

2.3 Certificates & Secrets

Open Certificates & Secrets in the left menu. Create a new secret under client secrets. (Note: this token is visible once.). Save this somewhere temporarily.

2.4 API Permissions

Now click on ‘API Permissions’. Press ‘Add a permission’, then select the following permissions:



API / Permissions name	Type	Description	Admin consent requ...	Status	
∨ Microsoft Graph (3)					···
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for 4CEE	···
Group.Read.All	Application	Read all groups	Yes	✓ Granted for 4CEE	···
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for 4CEE	···

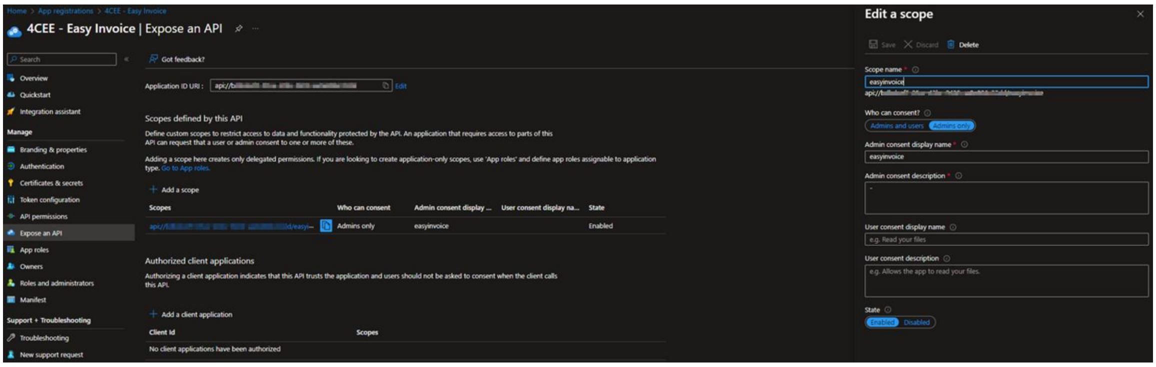
Figure 2: API Permissions

With these rights, you must pay attention to whether you select Application’ or ‘Delegated’ rights. Press Grant Admin consent for X. (Note: You need Global Administrator permissions to Grant admin consent.)

2.5 Scope

Open the menu item 'Expose an API' and click on ‘Add a scope’. Add a scope in accordance with the settings below.

Preference to use 'easyinvoice' for the scope name of the production environment of Easy Invoice. For the Easy Invoice testenvironment this should be 'easyinvoice_test'.



4CEE - Easy Invoice | Expose an API

Application ID URI : api://[redacted] Edit

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. Go to App roles.

+ Add a scope

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
api://[redacted]d/easyi...	Admins only	easyinvoice		Enabled

Authorized client applications

Authorizing a client application indicates that this API trusts the application and users should not be asked to consent when the client calls this API.

+ Add a client application

Client Id	Scopes
No client applications have been authorized	

Edit a scope

Scope name *: easyinvoice
api://[redacted]

Who can consent? Admins and users [✓ Admins only]

Admin consent display name *: easyinvoice

Admin consent description *: -

User consent display name: e.g. Read your files

User consent description: e.g. Allows the app to read your files.

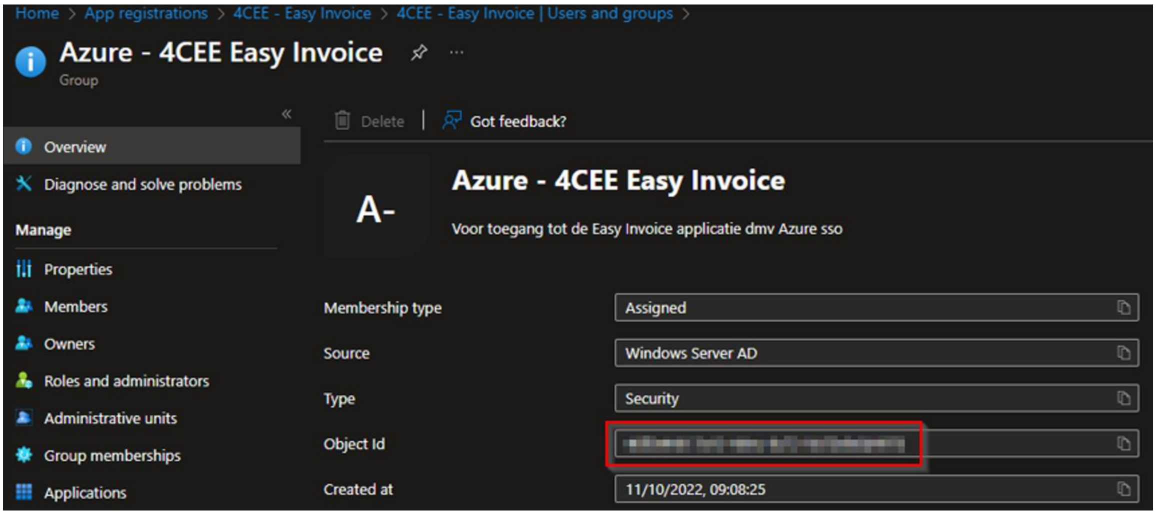
State: [✓ Enabled] Disabled

Figure 3: Expose an API

2.6 Groups

To be able to log in to Easy Invoice, users must be synchronized from Microsoft Entra ID. This is done using a group, this group (if not yet created, will have to be created first) must contain all users who need access to Easy Invoice.

Groups can be found in Microsoft Entra ID. The Object ID is related to a specific Group in Entra ID. This Object should be provided to the Easy Systems consultant. Note: The specific Easy Systems user should be included in this Group.



Azure - 4CEE Easy Invoice
Group

Azure - 4CEE Easy Invoice

Voor toegang tot de Easy Invoice applicatie dmv Azure sso

Membership type: Assigned

Source: Windows Server AD

Type: Security

Object Id: [redacted]

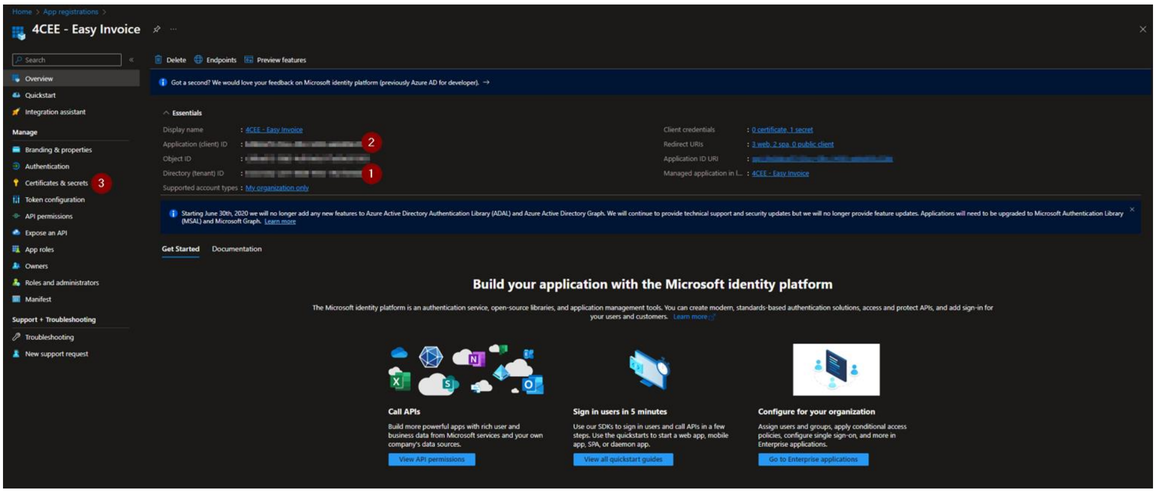
Created at: 11/10/2022, 09:08:25

Figure 4: Entra ID Group

3 Summary

The following information must be provided by the customer to the Easy Systems consultant.

- Tenant ID (see bullet 1)
- Client ID (see bullet 2)
- Client Secret (noted in paragraph 2.3 (see bullet 3))
- Group ID (paragraph 2.6)
- Active Directory Easy Systems User credentials
  - Username
  - Password
- Scope name (paragraph 2.5)



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Display name : 4CEE - Easy Invoice
Application (client) ID : [redacted]
Object ID : [redacted]
Directory (tenant) ID : [redacted]
Supported account types : My organization only

Client credentials : 0 certificate, 1 secret
Redirect URIs : 3 web, 2 spa, 0 public client
Application ID URI : [redacted]
Managed application in l... : 4CEE - Easy Invoice

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

Configure for your organization

Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.

Figure 5: Created App registration.