



LARMIA

ANVÄNDARHANDBOK
SSO

ANSVARSBEGRÄNSNING

All information i denna handbok har kontrollerats noggrant och bedöms vara korrekt. Emellertid lämnar Larmia Control AB inga garantier vad gäller manualens innehåll. Användare av denna manual ombeds rapportera felaktigheter, tvetydigheter eller oklarheter till Larmia Control AB, för eventuella korrigeringar i framtida utgåvor. Informationen i denna handbok kan ändras utan föregående meddelanden.

Mjukvaran som beskrivs i handboken levereras under licens från Larmia Control AB och får endast användas eller kopieras enligt licensvillkoren. Ingen del av denna bok får återges eller överföras i någon form eller på något sätt, elektroniskt eller mekaniskt, för något som helst ändamål utan uttryckligt skriftligt medgivande från Larmia Control AB.

COPYRIGHT

© Larmia Control AB. Med ensamrätt.

VARUMÄRKEN

MS-DOS, Windows, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10 och Windows 11 är registrerade varumärken som tillhör Microsoft Corporation.

Andra produktnamn som förekommer i denna bok används enbart i identifieringssyfte och kan vara ägarens registrerade varumärken.

September 2025

Version: 25.9.1.1

Innehållsförteckning

SSO

Konfigurering Entra ID (Azure AD)

Appregistrering webserver

Appregistrering webbklient

Konfigurering Evo

Approller Användargrupper

Serverinställningar / Inställningar Azure AD

SSO

Vi stödjer idag SSO med Entra ID (tidigare Azure AD). Det är en lösning med OAuth 2.0 som bl.a. använder Microsofts egna bibliotek för autentisering, [MSAL](#). Det här kräver viss förkunskap inom Azure för att sätta upp första gången. Kontakta oss om det är första gången du ska använda funktionen.

Konfigurering Entra ID (Azure AD)

- Det behövs 2 st appregistreringar (1 för klient och 1 för API).
- Klient och webbserver behöver åtkomst till `https://login.microsoftonline.com`.

Appregistrering webbserver

Optional claim

Behöver "optional claim" `groups`.

Home > App registrations > SsoApi

SsoApi | Token configuration

Search Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration**
 - API permissions
 - Expose an API
 - App roles

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim + Add groups claim

Claim ↑↓	Description	Token type ↑↓
groups	Optional formatting for group claims	ID, Access, SAML

Exponera scope

Behöver exponera ett "scope". Valfritt vad den kallas, men detta blir det som fylls i under `Scope webbklient` i Evo, samt används i appregistreringen för webbklienten.

Search

Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API** ☆
 - App roles

Application ID URI : 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 disp...	User cons
api://bf8423f8-944f-4e6b-aac7-4a2c56f...	Admins only	Test	

Behörigheter

Se till att dessa behörigheter finns:

Search

Refresh | Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions**
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting

⚠ Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

ℹ The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for MSFT

API / Permissions name	Type	Description	Admin con
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	No

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications.](#)

Appregistrering webbklient

Optional claim

Appregistreringen för klient behöver optional claim `login-hint` :

Home > App registrations > SsoClient

SsoClient | Token configuration

Search Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration**
 - API permissions
 - Expose an API

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim + Add groups claim

Claim ↑↓	Description	Token type ↑↓	Optional settings
login_hint	Login hint	ID	-

Behörigheter

Se till att dessa behörigheter finns:

Home > App registrations > SsoClient

SsoClient | API permissions

Search Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions**
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
 - Support + Troubleshooting

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for MSFT

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for MSFT
openid	Delegated	Sign users in	No	Granted for MSFT
User.Read	Delegated	Sign in and read user profile	No	Granted for MSFT
SsoApi (1)				
Test	Delegated	Test	Yes	Granted for MSFT

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Redirect

Lägg till `Single page application` redirect URI, t.ex. datornamn eller IP där klienten körs:

SsoClient | Authentication

Search

Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication**
 - Certificates & secrets
 - Token configuration
 - API permissions

Platform configurations

Depending on the platform or redirect URIs, specific authenticat

+ Add a platform

Single-page applicati

Redirect URIs

The URIs we will accept as de authenticating or signing out listed here. Also referred to a

https://localhost:7210/autl

Configure platforms



Web applications

Web
Build, host, and deploy a web server application. .NET, Java, Python

Single-page application
Configure browser client applications and progressive web applications. Javascript.



Mobile and desktop applications

iOS / macOS
Objective-C, Swift, Xamarin

Android
Java, Kotlin, Xamarin

Configure single-page application



< All platforms

Quickstart Docs

i The latest version of MSAL.js uses the authorization code flow with PKCE and CORS. [Learn more](#)

* Redirect URIs

Depending on the platform, such as redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

+ Add a platform

https://1.2.3.4 ✓

Grant types

MSAL.js 2.0 does not support implicit grant. Enable implicit grant settings only if your app is using MSAL.js 1.0. [Learn more about auth code flow](#)

✓ Your Redirect URI is eligible for the Authorization Code Flow with PKCE.

Single-Redirect

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https://1.2.3.4

https://1.2.3.4

https://1.2.3.4

https://1.2.3.4

https://1.2.3.4

http://1.2.3.4

http://1.2.3.4

Add URI

Grant type

✓ Your Redirect URI is eligible for the Authorization Code Flow with PKCE.

Front-channel

This is where single sign-on

Save

Configure

Cancel

Övrigt

Se till att resterande värden överensstämmer med bilden:

× ‹
🗨️ Got feedback?

- 🏠 Overview
- 📖 Quickstart
- 🔧 Integration assistant
- 🔍 Diagnose and solve problems
- ▼ Manage
 - 📄 Branding & properties
 - 🔑 Authentication
 - 🔑 Certificates & secrets
 - 📄 Token configuration
 - 🔑 API permissions
 - 📄 Expose an API
 - 👤 App roles
 - 👤 Owners
 - 👤 Roles and administrators
 - 📄 Manifest
- ▼ Support + Troubleshooting
 - 🗨️ New support request

Add URI

Grant types

✔️ Your Redirect URI is eligible for the Authorization Code Flow with PKCE.

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout
✔️

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

Select the tokens you would like to be issued by the authorization endpoint:

Access tokens (used for implicit flows)

ID tokens (used for implicit and hybrid flows)

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (MSFT only - Single tenant)

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

[Help me decide](#)

Konfigurering Evo

Approller-Användargrupper

För att koppla roller till en användargrupp behöver du lägga till roller i registreringen för webbservern. För att därefter kunna koppla ihop approller med användargrupper ska man gå till **Enterprise Application** i Azure och välja den appregistrering för webbserver/API man precis gjort och där koppla samman AD-grupper och approllen:

OBS! Du måste ha användare direkt under användargruppen i Entra, och inte ha nästlade behörigheter. Ett sätt att komma runt begränsningen är att skapa dynamiska grupper i Entra:

Hus adam Admin

Ändra

Namn:

Beskrivning:

Översiktsgrupp (ID-nummer, 0 = inaktiverad):

AD-identifierare (SSO-inställning):
 Approll Värde

Manuell styrning

- Ändra börvärde
- Ändra manöver
- Ändra mjukvarumanöver
- Ändra analog ut
- Forcera objekt
- Forcera från fjärr
- Tillåt tom kommentar

Larm

- Kvittera klass 0
- Kvittera klass A
- Kvittera klass B
- Kvittera klass C
- Kvittera klass D
- Kvittera klass E
- Kvittera klass F

I Server API:et skapas olika roller. Varje roll kopplas till en Användargrupp i Evo BMS. Det är approllens "värde" och användargruppens "AD-identifierare" som kopplas ihop.

Start > SsoApi

SsoApi | Approller

Skicka en approll | Har du någon feedback?

Översikt

Snabbstart

Integrationsassistenten

Diagnostisera och lös problem

Häntera

- Anpassning och egenskaper
- Autentisering
- Certifikat och hemligheter
- Tokenkonfiguration
- API-behörigheter
- Exponera ett API
- Approller**
- Ågare

Approller

Approller är anpassade roller för tilldelning av behörigheter till användare och appar. Programmet definierar och publicerar approllerna och tolkar dem som behörigheter under auktoriseringen.

Hur jag tilldelar approller

Visningsnamn	Beskrivning	Tillåtna medlemstyper	Värde	Id	Tillstånd
hus-cesar-jour	hus-cesar-jour	Användare/grupper	hus-cesar-jour	012f6f97-c8c1-405a-8...	Aktiverat
hus-cesar-drift	hus-cesar-drift	Användare/grupper	hus-cesar-drift	2dab2030-0a65-4974-...	Aktiverat
hus-cesar-admin	hus-cesar-admin	Användare/grupper	hus-cesar-admin	9aff3aee-6326-4b21-a...	Aktiverat
hus-beretil-jour	hus-beretil-jour	Användare/grupper	hus-beretil-jour	3e4070ef-a12c-40e3-a...	Aktiverat
hus-beretil-drift	hus-beretil-drift	Användare/grupper	hus-beretil-drift	b3a0757c-70ec-432d-...	Aktiverat
hus-beretil-admin	hus-beretil-admin	Användare/grupper	hus-beretil-admin	431c020b-24ec-484c-...	Aktiverat
hus-adam-jour	hus-adam-jour	Användare/grupper	hus-adam-jour	6e8d0a9a-89d9-401a-...	Aktiverat
hus-adam-drift	hus-adam-drift	Användare/grupper	hus-adam-drift	5effc563-7c51-434f-9...	Aktiverat

Redigera approll

Ta bort

Visningsnamn *

Tillåtna medlemstyper * Användare/grupper Program Båda (användare/grupper + program)

Värde * **AD-identifierare**

Beskrivning *

Vill du aktivera den här approllen?

Serverinställningar / Inställningar Azure AD

Serverkörning	Webbserver	Azure AD	PropTechOS
Klient-ID webbklient		76dde0d7-9375-4d19-b90	
Scope webbklient		api://bf8423f8-944f-4e6b-a	
Klient-ID webbserver		bf8423f8-944f-4e6b-aac7-	
Instans		https://login.microsoftonlir	
Tenant-ID		c9325040-a368-41d5-b7ad	

Inställning	Beskrivning
Klient-ID webbklient	Program-ID (Client-ID) för webbklientens appregistrering
Scope webbklient	Webbklientens API-behörighet (t.ex. <code>api://"guid"/namn</code>)
Klient-ID webbserver	Program-ID (Client-ID) för webbserverns appregistrering
Instans	URL till inloggning (t.ex. <code>https://login.microsoftonline.com/</code>)
Tenant-ID	Katalog-ID (Tenant-ID) för webbklientens appregistrering

Microsoft Azure Sök resurser, tjänster och dokument (G+)

Start >

SsoClient

Sök Ta bort Slutpunkter Förhandsversionsfunktioner

- Översikt
- Snabbstart
- Integrationsassistenten
- Diagnostisera och lös problem
- Hantera
 - Anpassning och egenskaper
 - Autentisering
 - Certifikat och hemligheter

Information

Visningsnamn : [SsoClient](#)

Program-ID (klient) : 76dde0d7-9375-4d19-b90 Klient-ID webbklient

Objekt-ID : ea9b147b-9ab8-45bb-a4c7

Katalog-ID (klientorganis... : c9325040-a368-41d5-b7ad Tenant-ID

Kontotyper som stöds : [Endast min organisation](#)

i Från och med 30 juni 2020 lägger vi inte längre till några nya funktioner i ADAL (Azure Active Directory Auth) tillhandahåller inte längre några funktionsuppdateringar. Programmen måste uppdateras till MSAL (Micros

SsoClient | API-behörigheter

Sök Uppdatera Har du någon feedback?

- Översikt
- Snabbstart
- Integrationsassistenten
- Diagnostisera och lös problem
- Hantera
 - Anpassning och egenskaper
 - Autentisering
 - Certifikat och hemligheter
 - Tokenkonfiguration
 - API-behörigheter
 - Exponera ett API
 - Approller
 - Ägare
 - Roller och administratörer
 - Manifest
- Support och felsökning

Om du beviljar medgivande för hela klientorganisationen kan din egen räkning påverkas inte. [Läs mer](#)

I kolumnen Administratörsmedgivande krävs visas standard i din organisation eller i organisationer där den här appen

Konfigurerade behörigheter

Program har behörighet att anropa API:er när de beviljas behörigheter ska innehålla alla behörigheter som programmet

+ Lägg till en behörighet ✓ Bevilja administratörsgodk

Namn på API/behörigheter	Typ	Beskrivning
Microsoft Graph (4)		
SsoApi (1)		
Test	Delegerat	Test

Om du vill visa och hantera medgivandebehörigheter för ensk

Test

SsoApi

Ta bort behörighet

api://bf8423f8-944f-4e6b-aac7 /Test **Scope webbklient**

Resursapp-id

bf8423f8-944f-4e6b-aac7

Behörighets-id

a5db6274-95c7-4610-97b

Administratörsmedgivande krävs

Ja

Visningsnamn för administratörsmedgivande

Test

Beskrivning av administratörsmedgivande

Test

SsoApi

Sök Ta bort Slutpunkter Förhandsversionsfunktioner

- Översikt
- Snabbstart
- Integrationsassistenten
- Diagnostisera och lös problem
- Hantera
 - Anpassning och egenskaper
 - Autentisering
 - Certifikat och hemligheter
 - Tokenkonfiguration
 - API-behörigheter

Har du tid ett ögonblick? Vi skulle uppskatta din feedback om Microsoft Identity Platform (tidigare Azure AD för utve

Information

Visningsnamn : SsoApi
 Program-ID (klient) : bf8423f8-944f-4e6b-aac7
 Objekt-ID : ceaa465d-34f6-40ec-8374
 Katalog-ID (klientorganis... : c9325040-a368-
 Kontotyper som stöds : Endast min organisation

Klient-ID webbserver

Från och med 30 juni 2020 lägger vi inte längre till några nya funktioner i ADAL (Azure Active Directory Authentic Programmen måste uppdateras till MSAL (Microsoft Authentication Library) och Microsoft Graph. [Läs mer](#)