iBabs & AzureAD/Office365

Inhoudsopgave

VOORWOORD	3
KOPPELEN TBV INLOGGEN	5
KOPPELEN TBV INLOGGEN EN GEBRUIKERSSYNCHRONISATIE	7
KOPPELEN TBV INLOGGEN, SYNCHRONISATIE EN TOEGANG ONEDRIVE EN SHAREPOINT ONLINE	9
BEHEREN VAN DE GELEGDE KOPPELING	11

Voorwoord

Beste iBabs gebruiker,

Om iBabs beter te integreren in bestaande IT-omgevingen bestaat de mogelijkheid om iBabs te laten inloggen via AzureAD van Office365 en/of Azure. Vanuit iBabs kunnen we op 3 niveaus deze integratie ondersteunen:

- Logon: AzureAD/Office365 gebruiken om single signon te krijgen met de eigen en bestaande gebruikersnaam met wachtwoord. Voordeel hiervan is dat het beheer van gebruikers slechts op 1 plaats gedaan hoeft te worden.
- 2. Logon+Sync: De extra mogelijkheid om te synchroniseren met een specifieke groep in AzureAD/Office365. Hierdoor hoeven gebruikers aan de kant van iBabs ook niet meer aangemaakt te worden en worden gebruikers die de organisatie verlaten ook automatisch verwijderd uit iBabs. Verder hetzelfde als het eerste punt.
- 3. Logon+Sync+Docs: Extra de mogelijkheid om OneDrive en SharePoint Online te integreren in iBabs voor document selectie. Verder hetzelfde als het tweede punt.

In de toelichting op de volgende pagina wordt kort omschreven hoe de integratie met AzureAD/Office365 werkt. Dit is een omschrijving rechtstreeks afkomstig van Microsoft. Omdat dit een tekst van Microsoft is, is deze in het Engels. In de afbeelding kan het blokje "Web Application" worden gezien als iBabs en "Azure AD" de inlogpagina die u gewend bent te gebruiken in AzureAD of Office365.



Here's what you need to know about the various components shown in the diagram:

- Azure AD is the identity provider. The identity provider is responsible for verifying the identity of users and applications that exist in an organization's directory, and issues security tokens upon successful authentication of those users and applications.
- An application that wants to outsource authentication to Azure AD must be registered in Azure AD. Azure AD registers and uniquely identifies the app in the directory.
- Developers can use the open-source Azure AD authentication libraries to make authentication easy by handling the protocol details for you. For more info, see Azure AD v2.0 authentication libraries and v1.0 authentication libraries.
- Once a user has been authenticated, the application must validate the user's security token to ensure that authentication was successful. You can find quickstarts, tutorials, and code samples in a variety of languages and frameworks which show what the application must do.
- The flow of requests and responses for the authentication process is determined by the authentication protocol that you used, such as OAuth 2.0, OpenID Connect, WS-Federation, or SAML 2.0. For more info about protocols, see the Concepts > Protocols section of the documentation.

Koppelen tbv inloggen

De basis koppeling tussen iBabs en AzureAD/Office365 is deze koppeling waarin alleen het inloggen mogelijk is gemaakt. Om deze koppeling te laten werken is het van belang dat het emailadres van de gebruiker in iBabs gelijk is aan het emailadres in AzureAD of Office365. Of om meer exact te zijn, tijdens het inloggen in AzureAD richting iBabs, checkt iBabs of het emailadres in iBabs overeenkomt met het zgn. 'UserPrincipalName' uit AzureAD.

Om dit te laten werken is het nodig dat wij bij iBabs aangeven dat u gebruik wilt maken van de AzureAD inlog methode.

Stap 1: Mail naar <u>support@ibabs.eu</u> met de vraag om de basis AzureAD koppeling voor uw organisatie te activeren.

Alle users die in iBabs al een overeenkomstig emailadres hebben kunnen dan direct gebruik maken van de koppeling. Echter is het wel zo dat dan iedere gebruiker in Azure voor zichzelf aan moet geven dat het goed is dat iBabs en AzureAD samen mogen werken. Om dit centraal te regelen kunt u ook als beheerder van AzureAD een generieke consent geven.

Stap 2: Om te kunnen synchroniseren is een extra consent nodig naar AzureAD. Een beheerder van Azure moet hiervoor deze URL aanklikken en een consent geven:

https://login.microsoftonline.com/common/adminconsent?client_id= 15dc427c-db64-48db-8f11-9750bc896f11&redirect_uri=https://portal.ibabs.eu/

De rechten die daarvoor worden gevraagd zijn:

Home > App registrations > App registrations (Preview) > iBabs - API permissions				
iBabs - API permissions				\$ X
 « Wanage Branding Authentication 	API permissions Applications are authorized to use APIs by grant/deny access. + Add a permission API / PERMISSIONS NAME	y requesting permissions. Th TYPE	ese permissions show up during the consent proce DESCRIPTION	ess where users are given the opportunity to ADMIN CONSENT REQUIRED
Certificates & secrets API permissions	Active Directory Graph (1) User.Read Microsoft Graph (1)	Delegated	Sign in and read user profile	- 🥝 Granted for iBabs BV
 Expose an API Owners 	User.Read	Delegated	Sign in and read user profile	- 🤡 Granted for iBabs BV
Manifest Support + Troubleshooting	These are the permissions that this applic permissions dynamically through code. S	ation requests statically. You ee best practices for request	may also request user consent-able ing permissions	
 Troubleshooting New support request 	Grant consent As an administrator, you can grant conser that end users will not be shown a conser Grant admin consent for iBabs BV	nt on behalf of all users in th t screen when using the app	is directory. Granting admin consent for all users n lication.	neans

Het alternatief inloggen blokkeren (dus nog kunnen inloggen met het onderliggende iBabs account terwijl er een gesynchroniseerd AzureAD account is) kan worden ingeregeld door onze helpdesk. Stuur hiervoor een email naar <u>Support@ibabs.eu</u>.

Koppelen tbv inloggen en gebruikerssynchronisatie

Voor het gebruik van de iBabs AzureSync is het nodig dat de organisatie al gebruikmaakt van de AzureAD login voor iBabs. De stappen om dit te activeren zijn eenvoudig.

ihah

Stap 1: Mail naar <u>support@ibabs.eu</u> met de vraag om de AzureSync voor uw organisatie te activeren.

Stap 2: Definieer zelf binnen AzureAD een groep tbv het synchroniseren met iBabs en voeg daar de gebruikers aan toe.

Stap 3: Om te kunnen synchroniseren is een extra consent nodig naar AzureAD. Een beheerder van Azure moet hiervoor deze URL aanklikken en een consent geven:

https://login.microsoftonline.com/common/adminconsent?client_id=3df93105-ca0f-4a5c-8abc-507c411e23a2&redirect_uri=https://portal.ibabs.eu/

De rechten die daarvoor worden gevraagd zijn:

Home > App registrations > App registrations (Preview) > iBabs User Sync - API permissions						
iBabs User Sync - API permissio	ons				;	☆ ×
≪ ₩ Overview ▲ Quickstart Manage	API permissions Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.					
Branding	API / PERMISSIONS NAME	ТҮРЕ	DESCRIPTION	ADMIN CONSENT RE	QUIRED	_
Authentication	▼ Azure Active Directory Graph (1)					-
Certificates & secrets API permissions	User.Read	Delegated	Sign in and read user profile	- 🤣 Granted	or iBabs B	v
 Expose an API 	▼ Microsoft Graph (5)					_
Owners	email	Delegated	View users' email address	- 🤣 Granted	for iBabs B	v
11 Manifest	Group.Read.All	Delegated	Read all groups	Yes 🤣 Granted i	for iBabs B	v
Support + Troubleshooting	openid	Delegated	Sign users in	- 🤡 Granted	for iBabs B	v
★ Troubleshooting	profile	Delegated	View users' basic profile	- 🤡 Granted	or iBabs B	V
New support request	User.Read	Delegated	Sign in and read user profile	- 🤣 Granted	or iBabs B	v
These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions						
	Grant consent					- 1
	As an administrator, you can grant consent on be that end users will not be shown a consent scree	enait of all users in th n when using the ap	is directory. Granting admin consent for all users means plication.			
	Grant admin consent for iBabs BV					

iBabs en AzureAD/Office365 11-2018 - pagina 7 van 11

Stap 4: Door het aanzetten van de AzureSync door iBabs support is er in Config-Instellingen een extra keuze gekomen. Ga naar Config->Instellingen om de groep in te stellen die gesynchroniseerd moet worden. Dit moet worden gedaan door een gebruiker met FB rechten in iBabs en beheer rechten in AzureAD.

Selecteer groep om te importeren.	ibabssync	¥

Stap 5: Daarna kan vanuit Config->Gebruikers de knop synchroniseren gebruiken. Hier zijn uiteraard iBabs functioneel beheer rechten voor nodig. Deze knop ziet er als volgt uit.



Na het drukken op de knop "Azure AD gebruikers synchroniseren" komt de volgende pop-up.

	Azure AD gebruikers synchronisatie	×	
lett	De Azure AD synchronisatie zal het volgende doen: 0 gebruikers toevoegen. 5 gebruikers updaten. 0 gebruikers verwijderen.		
;er	Klik op 'Synchroniseren' om de synchronisatie te starten. Klik op 'Annuleren' om de synchronisatie te annuleren.		
	Annuleren Synchroniser	en	@gi

Na synchronisatie wordt aangegeven hoeveel gebruikers zijn veranderd.

Momenteel is het nog niet mogelijk om automatisch een dagelijkse synchronisatie te doen. Dit heeft te maken met het goed en veilig organiseren van de benodigde rechten. We verwachten dat dit in het eerste half jaar van 2019 mogelijk zal gaan worden.

Het alternatief inloggen blokkeren (dus nog kunnen inloggen met het onderliggende iBabs account terwijl er een gesynchroniseerd AzureAD account is) kan worden ingeregeld door onze helpdesk. Stuur hiervoor een email naar <u>Support@ibabs.eu</u>.

Koppelen tbv Inloggen, synchronisatie en toegang OneDrive en SharePoint Online

Deze koppeling doet wat de 2 eerdere koppelingen ook mogelijk maken, echter is het hiermee ook mogelijk om op basis van DMS Services in iBabs gebruik te maken van uw OneDrive en SharePoint online documenten voor het samenstellen van agenda's. Om dit te activeren, doe het volgende:

Stap 1: Mail naar <u>support@ibabs.eu</u> met de vraag om de uitgebreide AzureAD koppeling voor uw organisatie te activeren. Indien u ook Sync wilt gebruiken, geef dit dan ook aan. Voor het instellen van de groepen om te syncen, zie het vorige hoofdstuk.

Stap 2: Om te kunnen synchroniseren is een extra consent nodig naar AzureAD. Een beheerder van Azure moet hiervoor deze URL aanklikken en een consent geven:

https://login.microsoftonline.com/common/adminconsent?client_id= fe14eaf5-00d5-4cdc-b6ded83043837d82&redirect_uri=https://portal.ibabs.eu/

De rechten die daarvoor worden gevraagd zijn:

Home > App registrations > App reg	istrations (Preview) > iBabsPlus - API permissions			
iBabsPlus - API permissions				\$
 Øverview Quickstart Manage 	API permissions Applications are authorized to use APIs by requ grant/deny access. + Add a permission	lesting permissions. Th	ese permissions show up during the consent process where r	users are given the opportunity to
🚾 Branding	API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
Authentication	✓ Azure Active Directory Graph (1)			
📍 Certificates & secrets	User.Read	Delegated	Sign in and read user profile	- 🥝 Granted for iBabs BV
API permissions	✓ Microsoft Graph (8)			
Service an API	email	Delegated	View users' email address	- 🤡 Granted for iBabs BV
Manifest	Files.Read	Delegated	Read user files	- 🤣 Granted for iBabs BV
Support + Troubleshooting	Files.Read.Selected	Delegated	Read files that the user selects (preview)	- 📀 Granted for iBabs BV
X Troubleshooting	Group.Read.All	Delegated	Read all groups	Yes 🥝 Granted for iBabs BV
New support request	openid	Delegated	Sign users in	- 🤡 Granted for iBabs BV
	profile	Delegated	View users' basic profile	- 🤣 Granted for iBabs BV
	Sites.Read.All	Delegated	Read items in all site collections	- 🤣 Granted for iBabs BV
	User.Read	Delegated	Sign in and read user profile	- 🤣 Granted for iBabs BV
	▼ SharePoint (6)			
	AllSites.Read	Delegated	Read items in all site collections	- 🤣 Granted for iBabs BV
	MyFiles.Read	Delegated	Read user files	- 🤣 Granted for iBabs BV
	MyFiles.Write	Delegated	Read and write user files	- 🥑 Granted for iBabs BV
	Sites.Search.All	Delegated	Run search queries as a user	Yes 📀 Granted for iBabs BV
	TermStore.Read.All	Delegated	Read managed metadata	Yes 🥑 Granted for iBabs BV
	User.Read.All	Delegated	Read user profiles	Yes 🥑 Granted for iBabs BV
	These are the permissions that this application permissions dynamically through code. See be	requests statically. You st practices for request	may also request user consent-able ing permissions	
	Grant consent			
	As an administrator, you can grant consent on that end users will not be shown a consent scre	behalf of all users in th een when using the app	is directory. Granting admin consent for all users means lication.	
	Grant admin consent for iBabs BV			

<ibabs>

Om daadwerkelijk gebruik te kunnen maken van de DMS Services, dient u apart contact op te nemen met iBabs om dit samen met u in te stellen.

Het alternatief inloggen blokkeren (dus nog kunnen inloggen met het onderliggende iBabs account terwijl er een gesynchroniseerd AzureAD account is) kan worden ingeregeld door onze helpdesk. Stuur hiervoor een email naar <u>Support@ibabs.eu</u>.

Beheren van de gerealiseerde koppeling

Als de consent is gegeven voor de bij uw organisatie benodigde applicatie, is er eigenlijk niet veel meer zichtbaar. AzureAD vertrouwt vanaf de consent voor uw organisatie iBabs als applicatie.

Om inzicht te krijgen in de gelegde koppeling dient u in te loggen op <u>https://portal.azure.com/</u> en vervolgens naar "Enterprise applications" binnen Azure te gaan. Daar zult u een overzicht treffen met alle door uw organisatie toegestane applicaties, waaronder iBabs.

Afhankelijk van de consent op 1 van de 3 iBabs applicaties treft u daar "iBabs", "iBabs User Sync" of "iBabs Plus". Dit geeft het volgende beeld:

Home > Enterprise applications - All applic	cations > iBabs - Overview
iBabs - Overview	
«	🔟 Delete
Overview	
🥳 Getting started	3
Manage	
Properties	
🗳 Owners	
x ^e Users and groups	
Provisioning	App usage between 10/23/2018 and 11/22/2018
Application proxy	1,500 IBABS
Self-service	
Security	1,000
Conditional Access	
\lambda Permissions	500
Activity	
Sign-ins	0
Audit logs	Oct 28 Nov 4 Nov 11 Nov 18 iBabs
Troubleshooting + Support	O sign-ins
🗙 Troubleshoot	
New support request	

Heel veel is daar niet op in te stellen, maar mocht u willen besluiten de eerder gegeven toegang (consent) als beheerder in te trekken, dan kan dat eenvoudig door boven aan de pagina op de knop "Delete" te klikken. Zodra deze is verwijderd zal iBabs niet meer via uw gebruikers uit AzureAD/Office365 in kunnen loggen in iBabs.