

Handleiding ParnasSys configureren voor Single- sign-on met Azure AD

van ParnasSys



Copyright © Topicus.Education B.V. Niets uit deze uitgave mag worden veeelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door print-outs, kopieën, of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van Topicus.Education B.V.

Versie: 4.34

Datum laatste aanpassing: 18-09-2024

Inhoudsopgave

Inhoudsopgave	2
1 Inleiding	3
2 Technische en functionele voorbereiding	3
2.1 Bovenschoolse organisatie	3
2.2 Azure AD feature laten activeren	3
2.3 Bovenschoolse accounts instellen	3
3 Stappenplan	4
3.1 Configuratie	4
3.2 Het eerste account koppelen	5
Account koppelen / User identifier koppelen	5
Azure SSO testen	6
3.3 (Optioneel) – Admin-consent geven	7
3.4 ParnasSys-accounts koppelen aan Azure-accounts	7
Manier 1 – semiautomatisch	7
Manier 2 – volledig handmatig	9
3.5 Azure login link	10
3.6 Instellen van de filepicker	11
3.7 Tot slot: oude inloggegevens en hulp van de ParnasSys servicedesk	11

1 Inleiding

Deze handleiding beschrijft stap voor stap hoe je de koppeling tussen ParnasSys en de Azure AD moet inregelen, zodat je deze kunt gebruiken als single sign on (SSO)-oplossing. Eerst wordt de koppeling geconfigureerd en daarna worden de medewerker-accounts gekoppeld. Vervolgens is de koppeling klaar om gebruikt te worden.

2 Technische en functionele voorbereiding

In dit hoofdstuk worden enkele punten gecontroleerd die geregeld moeten zijn voor de ParnasSys-omgeving waar de SSO-koppeling gebruikt gaat worden.

2.1 Bovenschoolse organisatie

De functionaliteit voor de Azure AD koppeling is alleen beschikbaar voor bovenschoolse organisaties (zoals besturen) met een bovenschoolse omgeving. Heb je deze nog niet, neem dan contact op met je ParnasSys-relatiebeheerder. (relatiebeheer@parnassys.nl)

2.2 Azure AD feature laten activeren

Om van de Azure AD-koppeling gebruik te kunnen maken, moet deze module eerst geactiveerd worden voor jouw bovenschoolse omgeving. De koppeling kan worden besteld via <https://www.parnassys.nl/producten/microsoft> of Neem contact op via relatiebeheer@parnassys.nl

2.3 Bovenschoolse accounts instellen

De accounts die voor de Azure SSO-koppeling gebruikt gaan worden, kunnen het beste bovenschools geregistreerd staan. In [dit artikel](#) vind je meer uitleg over de werking en het beheren van bovenschoolse accounts.

Staan de accounts nog niet bovenschools, dan vind je in [dit artikel](#) uitleg over het verplaatsen van schoolaccounts naar de bovenschoolse omgeving.

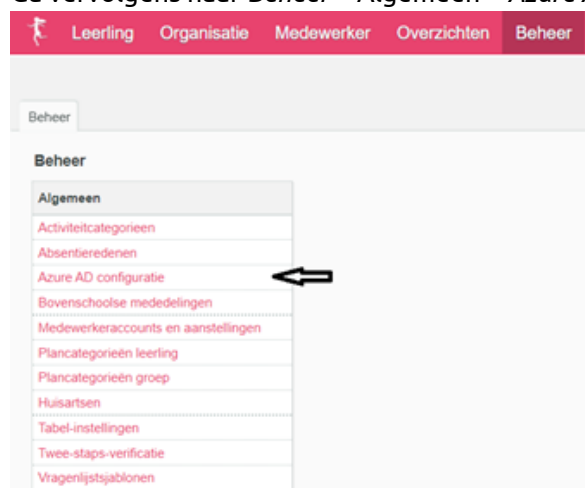
3 Stappenplan

3.1 Configuratie

Log in ParnasSys in met een account dat toegang heeft tot de bovenschoolse organisatie waar Azure aan gekoppeld gaat worden. Dit account moet de rol *Monitororganisatie-beheerder* of *Monitororganisatie-stafmedewerker (plus)* hebben.

Als er met een account ingelogd wordt dat aan meerdere organisaties gekoppeld is, controleer dan of rechts onderin je scherm de bovenschoolse organisatie geselecteerd staat (rechts van *Wijzig organisatie* moet de naam van de bovenschoolse organisatie staan).

Ga vervolgens naar *Beheer > Algemeen > Azure AD configuratie*.



Het is mogelijk om één of meerdere Azure AD-domeinen toe te voegen.

Klik op de knop *Toevoegen* onder in beeld. Het volgende scherm wordt weergegeven:

Azure AD configuratie toevoegen

Tenant ID	
Domain	<input type="text"/>
User filter	<input type="text"/>

Vul bij *Domain* het Azure AD-domein van jouw Azure-omgeving in en klik op *Opslaan*. Het *Tenant ID* wordt automatisch opgehaald. Het veld *User filter* is op dit moment niet belangrijk.

Na het opslaan zie je het volgende scherm:

Azure AD configuratie

Tenant ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Domain	xxxxxxxxxxxxxxxxxxxxxxxxxxxx
User filter	
Azure login link	https://inloggen.parnassys.net/idp/azure/xxxxxxxxxxxxxxxxxxxxxxxxxxxx
Admin consent	Geef consent voor alle gebruikers binnen tenant

De koppeling met Azure AD is nu succesvol ingeregeld. Over de velden *User filter*, *Azure login link* en *Admin consent* wordt verderop in deze handleiding meer uitleg gegeven.

3.2 Het eerste account koppelen

Account koppelen / User identifier koppelen

Nu de koppeling met de Azure AD ingeregeld is, koppel je eerst één ParnasSys-account met zijn Azure-AD-account, zodat je met dat account de SSO-koppeling kunt testen. Ga hiervoor naar de tab *Medewerker* en selecteer het account dat je wil koppelen. Het account dat je kiest, moet aan de volgende voorwaarden voldoen:

- Een account van een persoon met voldoende rechten binnen de Azure-omgeving.
 - Bij voorkeur dus met admin-rechten in Azure.
- Een account met een bovenschoolse aanstelling met de rol *Monitororganisatie-beheerder* of *Monitororganisatie stafmedewerker (plus)*
- Niet het account waar je nu mee ingelogd bent.
 - Als een account aan Azure gekoppeld is, kan dit account alleen maar via Microsoft SSO inloggen en niet meer met gebruikersnaam en wachtwoord op het ParnasSys-inlogscherf. Dus als je het account gebruikt waar je nu mee ingelogd bent en de SSO-koppeling werkt niet, dan heb je dat account buitengesloten.

Je kunt hiervoor natuurlijk ook een nieuw account aanmaken in de bovenschoolse omgeving.

Zodra je op het betreffende account geklikt hebt, ga je naar *Medewerker > Account*. Je ziet nu het volgende scherm:

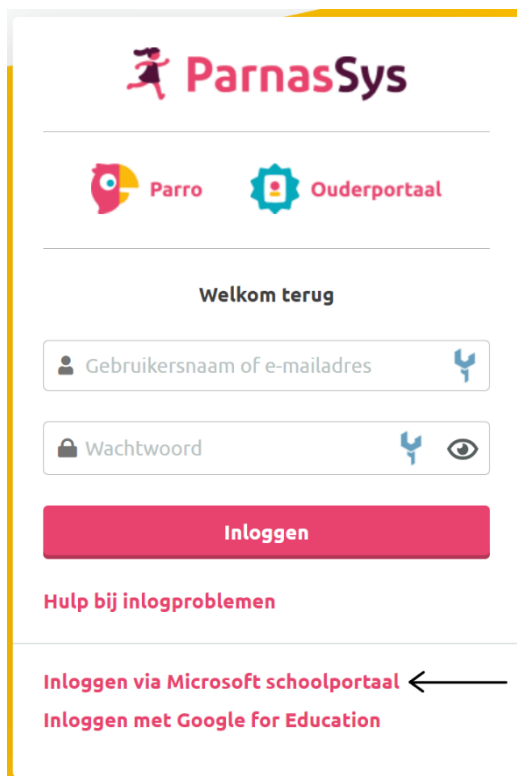
The screenshot shows the 'Account' management interface. At the top, there is a navigation bar with tabs: 'Leerling', 'Organisatie', 'Medewerker' (selected), 'Overzichten', and 'Beheer'. Below the navigation bar, the user's role is 'Monitororganisatie bt Beheerder'. There are three sub-tabs: 'Overzicht', 'Medewerker' (selected), and 'Aanstellingen'. The main content area is divided into three sections:

- Account**:
 - Contact e-mail: pssystemtest+1030@gmail.com (with an edit icon)
 - Account actief: Ja
 - E-mail uit ParnasSys ontvangen: Ja (with an information icon)
- ParnasSys ID**:
 - Gebruikersnaam: MONBH (with an information icon)
 - E-mail: pssystemtest+1030@gmail.com (with an information icon)
- Remote user identifier**:
 - Authentication provider: AZURE (with an edit icon)
 - User identifier: (empty field)

Klik op het bewerken-potlood achter *Remote user identifier*. In het volgende scherm kun je de User identifier van het Azure-account invullen dat je aan dit ParnasSys-account wil koppelen (deze vind je terug in de Azure-omgeving). Klik vervolgens op *Opslaan*.

Azure SSO testen

Log nu uit bij ParnasSys (knop rechts bovenin). Je komt weer op het inlogscherm.



ParnasSys

Parro Ouderportaal

Welkom terug

Gebruikersnaam of e-mailadres

Wachtwoord

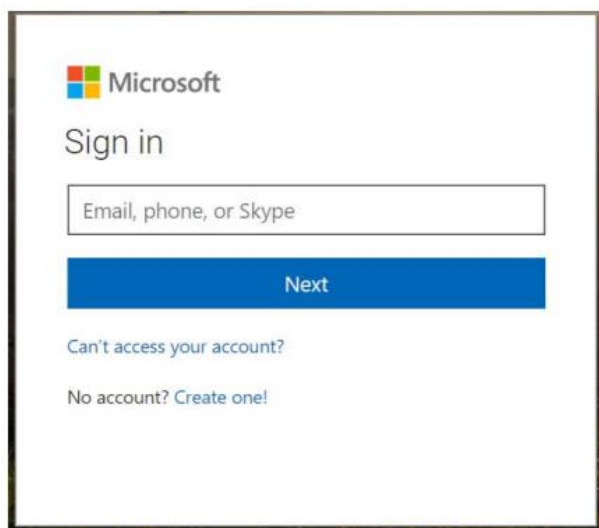
Inloggen

Hulp bij inlogproblemen

Inloggen via Microsoft schoolportaal ←

Inloggen met Google for Education

Klik op *Inloggen via Microsoft schoolportaal*. Je komt vervolgens op een Microsoft inlogscherm. Deze kan er als volgt uitzien of heeft wellicht al het design van jullie Azure-omgeving:



Microsoft

Sign in

Email, phone, or Skype

Next

Can't access your account?

No account? [Create one!](#)

Log vervolgens in bij Microsoft met het Azure-account dat je eerder koppelde aan een ParnasSys-account.

Als het inloggen helemaal afgerond is, moet je nu met het gekoppelde ParnasSys-account ingelogd zijn in ParnasSys. De koppeling is ingeregeld en werkt.

3.3 (Optioneel) – Admin-consent geven

Deze stap is optioneel, hieronder wordt uitgelegd waarom we dit aanraden en hoe je dit doet.

Bij het inloggen zojuist heb je ParnasSys toegang moeten geven tot enkele gegevens van de Azure-gebruiker. Deze gegevens zijn nodig om de juiste koppeling te leggen tussen het Azure-account en het ParnasSys-account. In technische termen heet dit *Consent geven*.

In principe krijgt elke gebruiker die van de SSO-koppeling gebruik gaat maken deze vraag. Dit kan verwarring opleveren bij de minder technische gebruikers binnen de organisatie. Om dit probleem te voorkomen, is het mogelijk om een Admin consent te geven. Met een Admin consent geef je in één keer toestemming voor alle gebruikers en zo voorkom je dat iedere gebruiker apart toestemming moet geven.

Voor de duidelijkheid: ParnasSys krijgt pas toegang tot de gegevens van de gebruiker als deze daadwerkelijk van de SSO-koppeling gebruik gaat maken.

Om Admin consent te geven, ga je in de bovenschoolse organisatie naar *Beheer > Algemeen > Azure AD configuratie*. Op dit scherm zie je een link *Admin consent*. Klik op deze link. Je komt nu bij Microsoft / Azure uit, waar je in één keer consent kan geven voor de hele tenant.

3.4 ParnasSys-accounts koppelen aan Azure-accounts

Nu de koppeling geconfigureerd en getest is, is het zaak om de overige ParnasSys-accounts te koppelen aan de Azure-accounts. Dit kan op twee manieren.

Manier 1 – semiautomatisch

Deze manier werkt alleen als Admin-consent gegeven is (paragraaf 3.3). Anders is manier 2 de enige manier om accounts te koppelen. Heb je dit Admin-consent niet gegeven, dan krijg je de melding: ParnasSys heeft geen toestemming om de medewerkers uit Azure uit te lezen. Dit is op te lossen door Admin-consent te geven (bij *Beheer > Algemeen > Azure AD configuratie*).

Voorwaarde: zorg dat je in ParnasSys ingelogd bent met de Azure-AD SSO-koppeling bij een bovenschools account met voldoende rechten. Als je niet ingelogd bent via Azure, krijg je de melding: *Kon geen token ophalen voor Azure - deze is benodigd voor het importeren. Is er wel via Azure ingelogd in ParnasSys?*

Klik op *Medewerker* en dan onderaan op de knop *Medewerkers importeren vanuit Azure*. Op het moment dat op deze knop wordt gedrukt, vraagt ParnasSys op de achtergrond de accounts uit de Azure-omgeving op (met een maximum van honderd Azure-accounts). Vervolgens wordt gekeken welk van deze Azure-accounts nog niet gekoppeld zijn aan een ParnasSys-account. Deze accounts worden op de volgende pagina weergegeven.

Let op!

Nadat je nieuwe medewerkers hebt geïmporteerd, zal je nog wel handmatig rollen moeten toevoegen aan de aanstellingen, anders kunnen de medewerkers niet inloggen.

Meerdere domeinen vastgelegd met verschillende tenants. Log in met een account behorend bij een andere tenant om gebruikers uit de andere tenant te zien.

Importeer medewerkers (Azure)

Hieronder is de lijst met medewerkers weergegeven waarvan het UPN (nog) niet bekend is in ParnasSys. Er zijn 2 acties mogelijk:

- Azure-account koppelen aan bestaand ParnasSys-account**
 - Is het veld in de kolom "Account koppelen" ingevuld, en wil je inderdaad het betreffende Azure-account koppelen aan het betreffende ParnasSys-account? Zet dan het vinkje aan voor deze regel.
 - Is het veld in de kolom "Account koppelen" niet gevuld en wil je dit Azure-account koppelen aan een bestaand ParnasSys-account? Klik dan op het vergrootglas-icoon en selecteer vervolgens het gewenste ParnasSys-account. Vergeet niet om dan ook het vinkje aan het begin van deze regel aan te zetten.
- Nieuw account aanmaken**
 - Wil je voor het betreffende Azure-account een nieuw ParnasSys-account aanmaken (omdat de betreffende medewerker / gebruiker nog geen ParnasSys-account heeft, bijvoorbeeld omdat het een nieuwe medewerker is)? Zet dan alleen het vinkje aan.
- Zoeken naar een account bij Azure**
 - Het zoeken op deze pagina wordt direct gedaan in de Microsoft Azure uitgaat van het zoeken op het begin van een woord met de term die je invoert.
 - Voorbeeld: Als je op een achternaam zoekt met de term "Jan" dan zal je alle achternamen terug krijgen die met "Jan" beginnen (bijvoorbeeld Jansmans, Janssen, Janou etc.). Wil je zoeken op Janssen dan kun je niet "ans" invoeren; je krijgt alleen alle achternamen die beginnen met "ans" te zien.

Achternaam
 E-mailadres
 Toon Azure-accounts die overeenkomen met een ParnasSys-account
 UPN

<input type="checkbox"/>	Roepnaam	Achternaam	E-mails	UPN	Account koppelen
<input type="checkbox"/>	Bruut	Bruut	bruut@brut.nl	bruut@brut.nl	<input type="text" value="BruutBruut"/> <input type="button" value="Q"/>
<input type="checkbox"/>	Jansen	Jansen	jansen@jansen.nl	jansen@jansen.nl	<input type="text" value="Jansen van de Kemp"/> <input type="button" value="Q"/>
<input type="checkbox"/>	Kennedy	Kennedy	kennedy@kennedy.nl	kennedy@kennedy.nl	<input type="text" value="Kennedy Kennedy"/> <input type="button" value="Q"/>

De gegevens in de kolommen *Voornaam*, *Achternaam*, *E-mail* en *User identifier* zijn de gegevens zoals ParnasSys deze van Azure heeft ontvangen. ParnasSys heeft een poging gedaan om in ParnasSys een bijbehorend account te vinden. Dit gebeurt op basis van een complex fuzzy-match algoritme. Als ParnasSys een account gevonden heeft, staat dit account direct ingevuld in de kolom *Account koppelen*.

Nu kun je hier twee acties uitvoeren:

- Account koppelen aan bestaand ParnasSys-account
 - Is het veld in de kolom *Account koppelen* ingevuld en wil je inderdaad het betreffende Azure-account koppelen aan het betreffende ParnasSys-account? Zet dan het vinkje aan voor deze regel.
 - Is het veld in de kolom *Account koppelen* niet gevuld en wil je dit Azure-account koppelen aan een bestaand ParnasSys-account? Klik dan op het vergrootglas en selecteer vervolgens het gewenste ParnasSys-account. Vergeet niet om dan ook het vinkje aan het begin van deze regel aan te zetten.
- Nieuw account aanmaken
 - Wil je voor het betreffende Azure-account een nieuw ParnasSys-account aanmaken (omdat de betreffende medewerker/gebruiker nog geen ParnasSys-account heeft, bijvoorbeeld omdat het een nieuwe medewerker is)? Zet dan alleen het vinkje aan.

Als je dit gedaan hebt, klik je op de knop *Importeren* en worden de acties uitgevoerd.

Let wel op bij nieuwe accounts: Aanstellingen en rollen worden niet automatisch aangemaakt / gekoppeld. Dit moet je achteraf nog handmatig uitvoeren in ParnasSys.

LET OP: Heb je in Azure ook leerling accounts staan? Deze haalt ParnasSys standaard ook op. Via *Beheer > Azure AD Configuratie* kun je een query invoeren bij je domein in het veld *User filter*

Beheer

Azure AD configuratie bewerken

Tenant ID

Domain

User filter

Deze query ziet er ongeveer zo uit: (Let op dit is een voorbeeld en zal bij jullie bestuur niet werken. Vraag aan de organisatie die jullie Azure beheert welke query jullie moeten gebruiken).

assignedLicenses/any(s:s/skuld eq a403e1-...-5c235)

Wanneer je de -voor jullie- juiste query invoert, zal ParnasSys automatisch alleen medewerkers ophalen uit Azure en de leerling accounts negeren.

Manier 2 – volledig handmatig

De tweede manier is eigenlijk gelijk aan hoe het eerste account (in stap 2) is gekoppeld:

Ga naar de medewerker-zoeken-pagina. Zoek de medewerker op waarvan je het ParnasSys-account aan een Azure-account wil koppelen. Klik op de medewerker, ga naar *Medewerker > Account*. Je ziet nu het volgende scherm:

Account		
Contact e-mail		psysmailtest+1030@gmail.com
Account actief		Ja
E-mail uit ParnasSys ontvangen		Ja

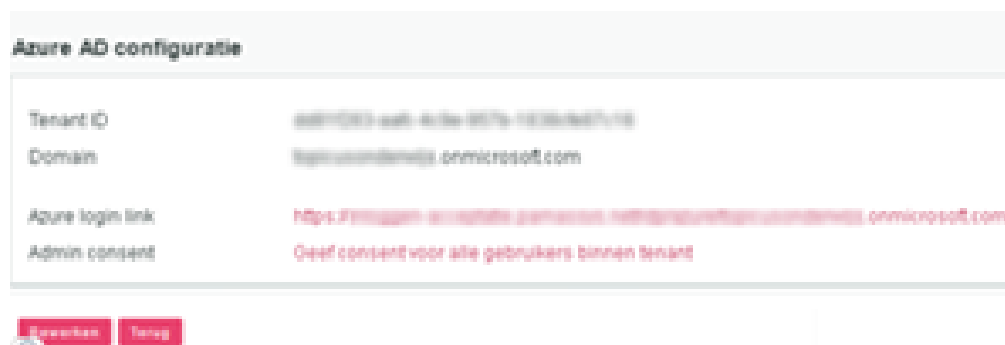
ParnasSys ID		
Gebruikersnaam		MONBH
E-mail		psysmailtest+1030@gmail.com

Remote user identifier		
Authentication provider		AZURE
User identifier		

Klik op het bewerken-potlood achter *Remote user identifier*. In het volgende scherm kun je de *User identifier* van het Azure-account invullen die je aan dit ParnasSys-account wil koppelen (deze vind je terug in de Azure-omgeving). Klik vervolgens op *Opslaan*.

3.5 Azure login link

In hoofdstuk 1, bij het configureren van de koppeling, zag je aan het eind van het hoofdstuk de *Azure login link*.



Waarvoor is deze link en wat kan je er mee? Deze login-link wordt gegenereerd op basis van het Azure-domein. Deze link kun je gebruiken in bookmarks, op webpagina's en in mailcommunicatie naar medewerkers die via Azure AD in willen loggen. Door het gebruik van deze link slaat de gebruiker de stap over waarbij de gebruiker op de ParnasSys-inlogpagina op de link *Inloggen via Microsoft schoolportaal* moet klikken. De gebruiker komt bij het gebruik van deze specifieke link direct op de inlogpagina van de juiste Azure-omgeving met de stijl en het thema welke daar ingesteld is.

3.6 Instellen van de filepicker

Als medewerkers zijn ingelogd via Azure kunnen zij links naar documenten uit de Sharepoint-omgeving van de school toevoegen aan het dossier van de leerling/groep in ParnasSys via een filepicker.

Om de filepicker te kunnen gebruiken, moet eerst worden ingesteld naar welke map in Sharepoint deze verwijst.

Dit stel je in op de pagina *Beheer > Algemeen > Azure AD configuratie*.

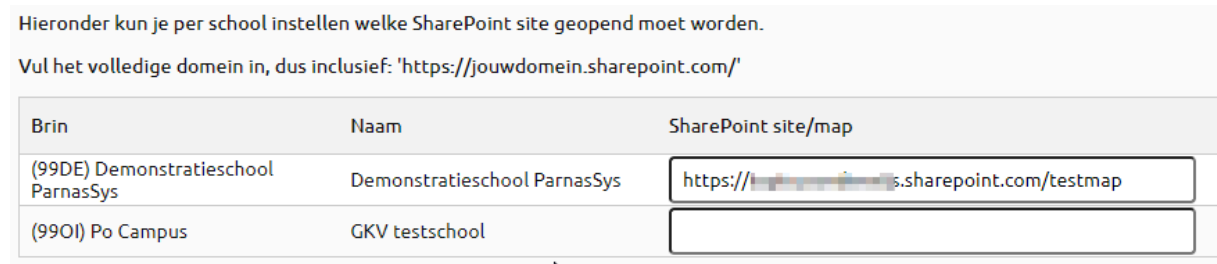


The screenshot shows the 'Beheer' (Management) section of the ParnasSys interface. It displays a table for 'Domains - 1 t/m 2 (van 2)'. Below this, there is a table for configuring SharePoint sites per school. The table has three columns: 'Brin', 'Naam', and 'SharePoint site/map'.

Brin	Naam	SharePoint site/map
(99DE) Demonstratieschool ParnasSys	Demonstratieschool ParnasSys	https://[redacted].sharepoint.com/testmap
(99OI) Po Campus	GKV testschool	

Klik op de regel van de BRIN.

Vul hier de URL in van jullie Sharepoint omgeving en klik op *Opslaan*.



This screenshot shows a form for configuring SharePoint sites. It includes a text input field for the URL, which is pre-filled with 'https://[redacted].sharepoint.com/testmap' for the first row. The second row has an empty input field.

Brin	Naam	SharePoint site/map
(99DE) Demonstratieschool ParnasSys	Demonstratieschool ParnasSys	https://[redacted].sharepoint.com/testmap
(99OI) Po Campus	GKV testschool	

3.7 Tot slot: oude inloggegevens en hulp van de ParnasSys servicedesk

Wanneer je bovenstaande stappen doorloopt is alles voorbereid voor je medewerkers om te werken met de single sign-on functionaliteit van Azure en de filepicker van Sharepoint.

Gebruikers zijn wellicht gewend om bij ParnasSys met hun ParnasSys-gebruikersnaam en -wachtwoord in te loggen. Echter, zodra een ParnasSys-account gekoppeld is aan een Azure-account, dan is het niet meer mogelijk om met de ParnasSys gebruikersnaam en wachtwoord-combinatie in te loggen. Het is dan alleen nog mogelijk om via de Azure-single-sign-on koppeling in te loggen.

Het kan in een klein aantal gevallen voorkomen dat jullie Azure omgeving anders is ingesteld dan in deze handleiding staat uitgelegd. Je kunt dit dan het beste bespreken met de ICT leverancier die Azure voor jullie instelt. De ParnasSys servicedesk wil je graag helpen met het inrichten van ParnasSys, zij hebben helaas niet de expertise om te helpen met de inrichting van jullie Azure of Sharepoint-omgeving. Mochten jullie verdere begeleiding willen, dan kun je het beste contact opnemen met **APS IT-diensten** (apsitdiensten.nl). Zij kunnen je uitgebreid begeleiden met de inregeling van de koppeling tussen ParnasSys en Azure.