Inloggen met LDAP (Active Directory)

Inleiding

Het is vaak gewenst dat gebruikers niet weer een nieuw wachtwoord hoeven te onthouden om in te loggen op het Zermelo Portal. Het controleren van de gebruikersnaam en het wachtwoord via LDAP is dan vaak een goede oplossing. Iedereen kan dan inloggen met hetzelfde wachtwoord als ze voor alle andere schoolsites gebruiken. Op het moment dat LDAP aan staat en een gebruiker inlogt, maakt het Portal verbinding met de LDAP-server van de school. Dit kan een aparte server zijn maar ook Active Directory (AD) heeft deze functionaliteit. Het Portal probeert dan als deze gebruiker in te loggen op deze server. Als dit lukt geeft het Portal de gebruiker toegang.

> **SAML**
>
> Als het ook mogelijk is om Single-sign-on met SAML 2.0 (Active Directory) in te stellen dan bevelen wij dit aan.

Op deze pagina

Zie ook

Stappenplan instellen LDAP

> We raden u ten zeerste aan om dit stappenplan te volgen. Als u dit niet doet dan lukt het waarschijnlijk niet om LDAP correct in te stellen. Als u contact opneemt is het eerste wat we u vragen of u dit stappenplan hebt doorlopen en bij welke stap u bent blijven steken. Stappen 1-3 zijn niet optioneel en kunnen niet worden overgeslagen.

1. Voor u begint

Voordat u begint met het instellingen van de koppeling heeft u de volgende personen nodig:

1. Iemand met toegang tot de LDAP/AD server (LDAP beheerder)
2. Iemand met rechten om de firewall aan te passen (firewall beheerder)
3. Iemand met "admin" rechten op het portal (portal admin)

Wij raden aan om met deze personen bij elkaar te gaan zitten om de koppeling in te richten. Op deze manier zijn de lijntjes kort en kan het stappenplan snel en soepel doorlopen worden.

Verder heeft u nodig:

1. De login gegevens van een docent (volgens de LDAP/AD server)
2. De login gegevens van een leerling (volgens de LDAP/AD server)

2. Toegang LDAP server instellen

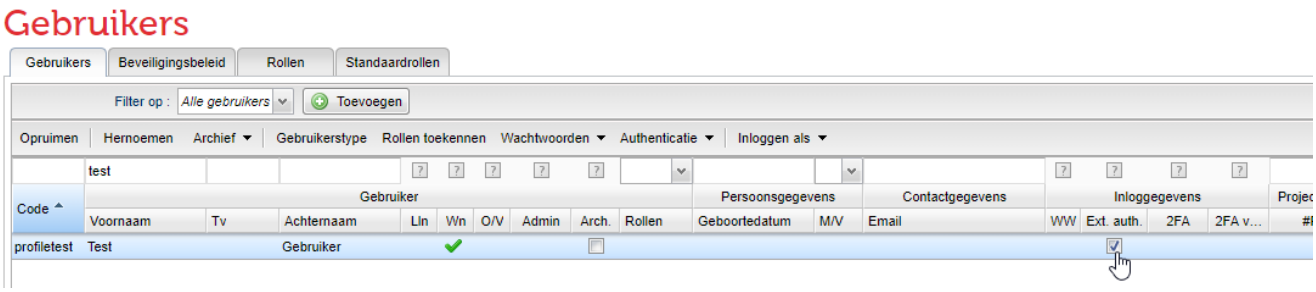
1. De firewall beheerder maakt in samenwerking met de LDAP beheerder de LDAP-server beschikbaar via internet voor de IP adressen van het Portal. Dit doen ze door de instellingen van uw eigen servers en firewalls aan te passen. De poort is de standaard LDAP poort 389, voor beveiliging maken we gebruik van STARTTLS. Het Portal ondersteunt LDAPv3 en mogelijk eerdere versies. Zie voor de IP adressen waar verbinding vanuit wordt gemaakt IP adressen.
2. Iemand met Admin rechten in het portal past in het portal (*Beheer > Admin-paneel > Instellingen)* de het volgende aan:
    a. ldap.enabled -> true
    b. ldap.host -> de hostname van de server (ldap.school.nl of een IP adres). **Als u een hostname gebruikt dient deze extern bekend te zijn via DNS.**
    c. ldap.port -> 389 (in zeldzame gevallen is dit een andere poort)
    d. ldap.tls.enabled -> false (we zorgen eerst dat het werkt zonder encryptie, later zetten we dit pas aan)

3. Inloggen mogelijk maken

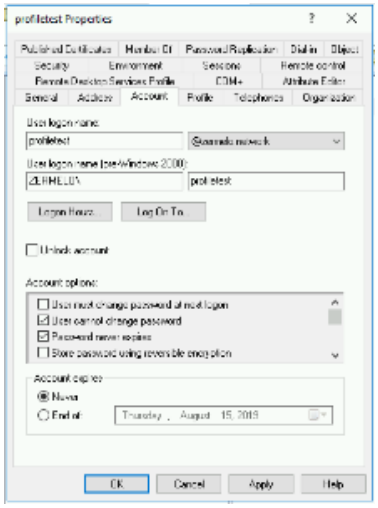
We gaan nu voor een testgebruiker zorgen dat deze kan inloggen via LDAP. In dit voorbeeld is dit de volgende docent:

Naam	Bob Whiler
Afkorting/code	WHI
Loginnaam die Bob op school gebruikt	bobw

Om te zorgen dat deze gebruiker kan inloggen zetten we allereerst het vinkje aan bij *Externe authenticatie* (voorheen *LDAP)* op de pagina *Beheer > Portal > Gebruikers*:

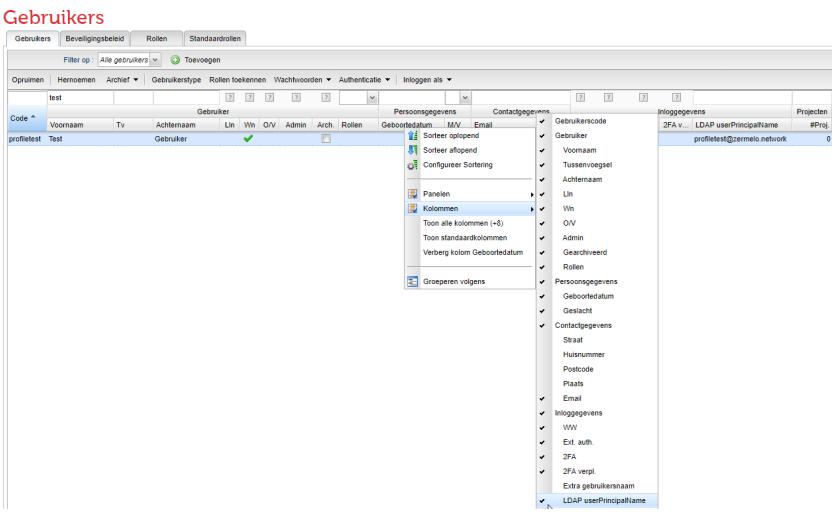


We moeten ook het veld *LDAP userPrincipalName* gaan vullen. Om te weten wat hier moet staan kijken we in de LDAP/Active Directory naar de eigenschappen van de gebruiker, onder *Account*.



In dit geval is de userPrincipalName "profiletest@zermelo.network". Dit vullen we in bij de kolom *LDAP userPrincipalName:*

De kolom LDAP userPricipalName brengen we in beeld door met rechts te klikken in een kolomkop, bijvoorbeeld 'Geboortedatum' en bij menu Kolommen te kiezen voor LDAP userPricipalName.



Nu kan deze gebruiker met zijn **afkorting** (profiletest) en standaard schoolwachtwoord inloggen. U kunt dit nu testen:

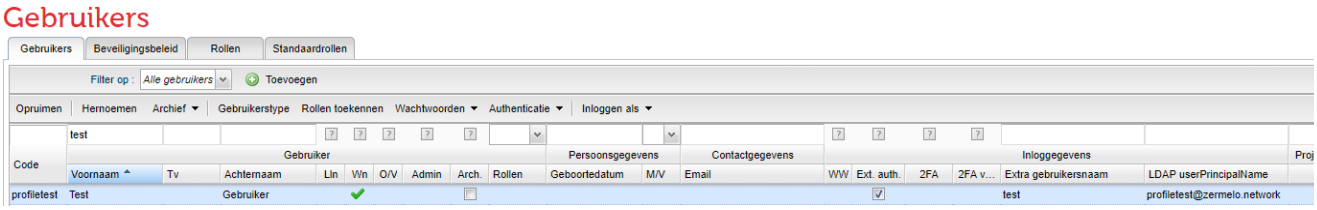
Als u dit werkt voor de testdocent kunt u hetzelfde proberen voor een testleerling. Het kan zijn dat u iets anders moet invullen als userPrincipalName.

> **Tip**
>
> U kunt met een programma als LDAPExplorerTool eerst op uw eigen netwerk proberen of het inloggen als leerling of docent met de bepaalde userPrincipalName goed werkt. U vult in dit programma bij de instellingen bij "User DN" de bepaalde userPrincipalName in. "Use SSL port" moet op "No" staan en eventueel kunt u later proberen of u "Use TLS" kunt aanzetten.

Lukt het niet om op deze manier iemand te laten inloggen? Als u contact opneemt kunnen wij u helpen door de gedetailleerde foutmeldingen te bekijken in onze logs. Het kan zijn dat het verbinding maken niet goed werkt of de gebruikersnaam waarmee de server probeert in te loggen op de LDAP server niet correct is.

4. Inloggen op het portal met een andere gebruikersnaam (optioneel)

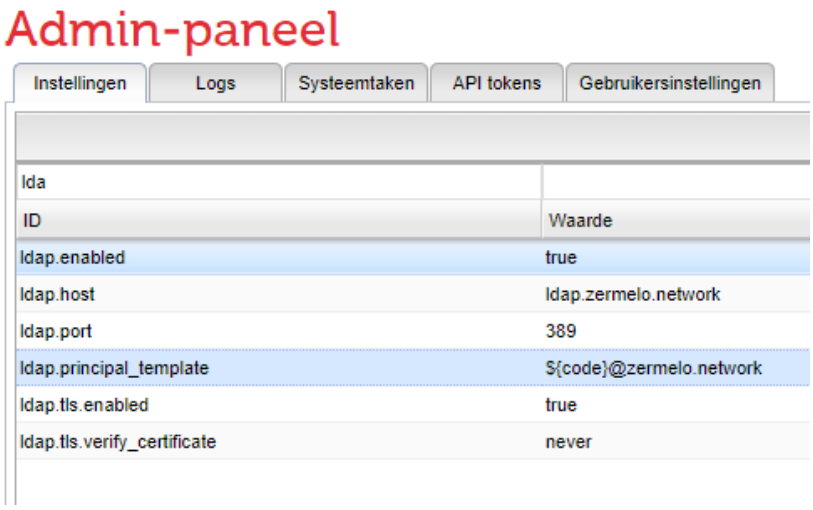
Nadat u stap 3 heeft afgerond kan een gebruiker inloggen op het portal met een standaard schoolwachtwoord. Als gebruikersnaam moet echter de de afkorting of leerlingnummer worden ingevoerd. Mogelijk wilt u dat leerlingen of docenten met een andere gebruikersnaam inloggen. Vooral voor docenten is dit vaak voorletter.achternaam. In dat geval kunt u deze gegevens inlezen in de kolom *Extra gebruikersnaam* (intern: `username`) . In het voorbeeld uit stap 3 wilt u misschien dat deze gebruiker gewoon kan inloggen met "test". U vult dan "test" in bij de kolom *Extra gebruikersnaam:*



Nu kan de gebruiker inloggen met "test" en zijn eigen wachtwoord:

5. LDAP voor meerdere gebruikers aanzetten (optioneel)

Als het lukt om zowel een leerling als een docent te laten inloggen kan de portal admin kijken of dit centraal in te stellen is voor alle gebruikers. Dat is een stuk makkelijker dan het voor alle gebruikers los instellen. U kunt de instelling `ldap.principal_template` gebruiken om aan de hand van de code, extra gebruikersnaam of mailadres automatisch de juiste userPrincipalName bij een gebruiker te laten genereren. Het kan bijvoorbeeld zijn dat u ziet dat u bij alle gebruikers een userPrincipalName hebt opgegeven die eindigt op "@rfs.local". Dit voelt een beetje dubbelop en kan meer werk zijn bij invoeren/importeren. In dat geval kunt u bij alle gebruikers de userPrincipalName kolom weer leegmaken en bij de instellingen het `principal_template` instellen op "${username}@rfs.local":

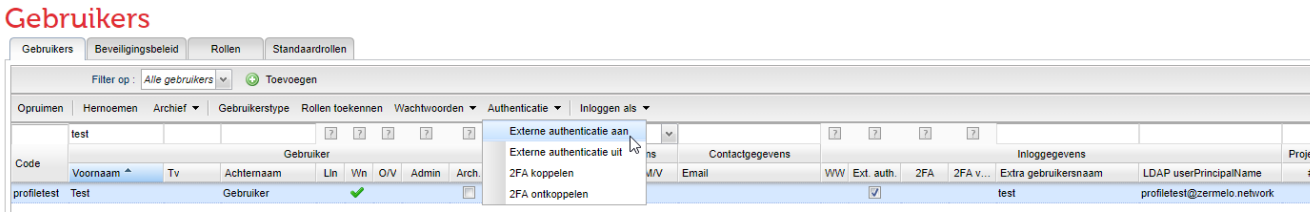


Nu hoeft u bij een nieuwe gebruiker alleen maar de Extra gebruikersnaam in te vullen en het vinkje *Externe authenticatie* (voorheen *LDAP*) aan te zetten. Let u er bij het testen op dat u de kolom *userPrincipalName* bij de testgebruiker leegmaakt, als u dat niet doet wordt namelijk het `principal_template` niet gebruikt voor deze gebruiker.

Het kan zijn dat het u niet lukt met behulp van de code, extra gebruikersnaam of mailadres een correcte login string te produceren voor de LDAP server. In dat geval moet u deze voor elke gebruiker inlezen in de kolom `userPrincipalName`. U kunt nog steeds iets in de kolom extra gebruikersnaam zetten zodat de gebruikers wel gewoon met hun standaard loginnaam kunnen inloggen op het portal.

Als de voorgaande stappen gelukt zijn is het nu mogelijk om bij meerdere gebruikers het vinkje *Externe authenticatie* (voorheen *LDAP*) aan te zetten zodat ze kunnen inloggen. Dit kan ook via het menu "LDAP" bij een aantal gebruikers tegelijk gebeuren:

Dit doet u door meerdere gebruikers te selecteren en via het menu Authenticatie te kiezen voor Externe authenticatie aan.



Deze gebruikers kunnen niet meer met het wachtwoord wat in het Portal staat inloggen maar alleen maar met het wachtwoord wat bij de LDAP-server bekend is. Ook kunnen deze gebruikers hun wachtwoord niet meer wijzigen.

LDAP niet voor alle gebruikers

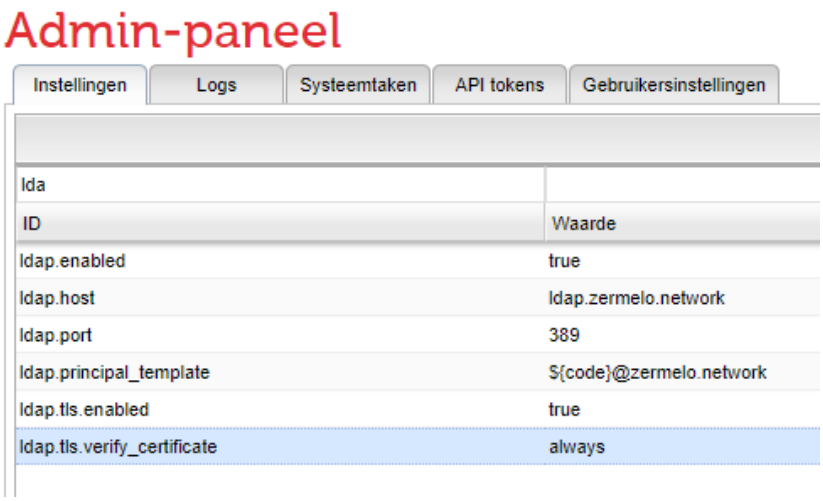
We raden aan om de admin account, (die met code admin) niet te koppelen aan LDAP om hier altijd op terug te kunnen vallen. Naast deze admin kunt u ook andere gebruikers buiten de LDAP koppeling houden door Ext. auth. uit te laten staan. Voor het gebruik van het testportal test-*uwschoolnaamhier*.zportal.nl is zo een gebruiker nodig omdat de LDAP niet werkt voor de testportal.

6. De LDAP verbinding beveiligen

Als alles werkt kunt u nu aanzetten dat er een beveiligde verbinding gebruikt moet worden.

1. U zet ldap.tls.enabled op "true" en ldap,tls.verify_certificate op "never". De verbinding is nu beveiligd maar in een zeldzaam geval zou een kwaadwillende een server van hemzelf zich kunnen laten voordoen als uw server, en dan de wachtwoorden kunnen bemachtigen.

2. U kunt kijken of het ook werkt met deze instelling op "always". In dat geval controleert onze server het beveiligingscertificaat van uw server. Dit werkt alleen als u de server benadert via een hostname en als dit certificaat ook geldig is. Een self-signed certificaat werkt dus niet.



Overzicht van instellingen

De volgende instellingen kunt u aanpassen onder *Beheer > Admin-paneel > Instellingen*

Let op: sommige instellingen zijn hoofdlettergevoelig. In geval van twijfel is het het beste om alles met kleine letters te schrijven.

Instelling	Voorbeeld	Toelichting
`ldap.enabled`	`true`	"true" als LDAP gebruikt mag worden, "false" als dit niet zo is.
`ldap.host`	`ldap.school.nl`	De hostname of IP adres van de LDAP server van de school.
`ldap.port`	`389`	De poort waarop verbinding gemaakt moet worden. Het portal ondersteunt alleen standaard LDAP (op poort 389) met als gewenst STARTTLS als beveiliging. LDAPS (standaard poort 636) wordt op dit moment niet ondersteund.
`ldap.principal_template`	`${code}@schoolnaam.local`	De principal waarmee Zermelo Portal probeert in te loggen op de LDAP-server. Gebruik ${code} voor de gebruikersnaam en ${email} voor het mailadres. Tevens kan ${username} worden gebruikt voor de apart ingestelde gebruikersnaam. **Als bij een gebruiker de `userPrincipalName` is ingesteld wordt deze gebruikt. De `principal_template` wordt dan genegeerd.**
`ldap.tls.enabled`	`true`	"true" als de verbinding beveiligd moet worden voor het versturen van de gebruikersnaam en het wachtwoord door middel van STARTTLS, anders "false".
`ldap.tls.verify_certificate`	`always`	"never" als het certificaat niet gecontroleerd moet worden, omdat het bijvoorbeeld self-signed is. "always" als het certificaat gecontroleerd moet worden en de verbinding moet worden afgebroken als er iets mis is. **Als er bij ldap.host een IP adres is ingevoerd dan moet deze instelling op "never" staan. Tevens werkt controle van het certificaat alleen als het een officieel en geldig certificaat is.**

UserPrincipalName

De *userPrincipalName* is waarschijnlijk de lastigste instelling. Voorbeelden van login namen voor LDAP zijn:

1. 1203446@leerling.school.nl
2. ll1203446@leerling.school
3. 1472346 (leerlingnummer)
4. voornaam.achternaam@school.local
5. CN=1234,OU=leerlingen,DC=schoolnaam,DC=local

Soms zitten leerlingen en medewerkers niet in de AD niet in één container, maar in verschillende. Het gebruik van de distinguishedName (CN=...) uit de AD is dan niet mogelijk. U kunt dan mogelijk gebruik maken van de userPrincipalName (1234@leerling.school).

IP adressen

Verbindingen met uw LDAP server worden gemaakt vanaf een beperkt aantal adressen. Op de pagina IP-adressen kunt u zien welke dat zijn.

Hulp bij het instellen van LDAP

Komt u er niet uit? Het instellen van LDAP is specialistisch werk waar we u niet direct telefonisch mee kunnen helpen. U kunt de volgende gegevens mailen naar helpdesk@zermelo.nl, wij nemen dan contact met u op.

1. Contactgegevens (email en telefoon)
2. Urgentie (wanneer moet LDAP werken?)
3. Portaladres
4. Wie moeten er kunnen inloggen via LDAP? Alleen leerlingen? Leerlingen en docenten?
5. Wat de laatste succesvolle afgeronde stap uit het stappenplan is.
6. Afkorting/leerlingnummers van gebruikers waar u voor geprobeerd heeft om LDAP in te stellen.