

Single Sign-On SSO for PowerSchool

PowerSchool supports the following methods for SSO:

- PowerSchool SIS as an Identity Provider (to sign on to other PowerSchool products)
- PowerSchool SIS as OIDC Service Provider for SSO
- PowerSchool SIS as SAML Service Provider

PowerSchool SIS as OIDC Service Provider for SSO

PowerSchool SIS supports external OpenID Connect (OIDC) identity providers (IdP), which allows authorized users to single sign-on (SSO) into the PowerSchool SIS using their identity provider and then seamlessly navigating to any of their PowerSchool products with that single set of credentials. Certified IdPs include Microsoft Azure and Google, which support Multi-Factor Authentication (MFA). Staff, Teachers, Students, and Parents user types are all supported.

In other words, you can setup PowerSchool to use your Azure or Google sign-on to login.

Documentation

Each version of PowerSchool has its own documentation revision. Search the built-in System Help for the term "OIDC", it should be the first link titled "PowerSchool SIS as OIDC Service Provider for SSO"

Frequent Questions

- Do all users have to use SSO if enabled?
 - No, you can selectively enable for just Staff, or Teachers, or Students, or Parents, or any combination of the above.

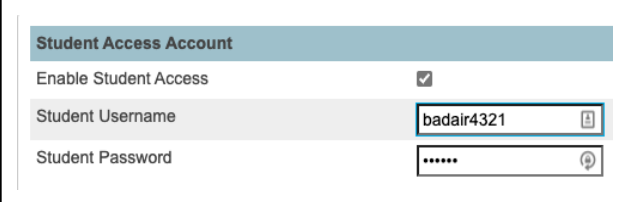

Enable OIDC Authentication for Staff Users	<input type="checkbox"/>
Enable OIDC Authentication for Teacher Users	<input type="checkbox"/>
Enable OIDC Authentication for Parent Users	<input type="checkbox"/>
Enable OIDC Authentication for Student Users	<input checked="" type="checkbox"/>

SSO

- Can some users in a group have SSO turned off?
 - No, once a group is enabled, all users in that group must use SSO
- How can I manage access for vendors, contractors, consultants, etc?
 - If you set your IDP option to public, the user can use any login from that platform. You could also create an account for them in Azure or Google. Example: If you use Google and you set it up as public on the Google side, you can enable login for anyone with a Gmail account.
- What happens if Google or Azure becomes unavailable?
 - Support can assist you with running a script that can turn off SSO in such an event.
- Do I have to reset a user's Google or Azure password if I need to use their account for troubleshooting, testing, or preparing documentation and training materials?
 - If you need to "impersonate" a user, you do not need to "take over" their account. you can temporarily just change their Global ID in PowerSchool to a different ID. Use that ID to login as them and when finished restore their Global ID.

Global ID

When you enable SSO, the user's "Username" and "Password" get replaced by a Global ID field, which is separate from their email address field. This requires you to have a process in place to populate that field during implementation and for onboarding as new users are added.

BEFORE	AFTER
 <p>Student Access Account</p> <p>Enable Student Access <input checked="" type="checkbox"/></p> <p>Student Username <input type="text" value="badair4321"/></p> <p>Student Password <input type="password" value="*****"/></p>	 <p>Student Access Account</p> <p>Enable Student Access <input checked="" type="checkbox"/></p> <p>Identity Provider Global ID <input type="text" value="badair4321@myschool.org"/></p>

- DEM/DIM have templates to help you export and import the Global ID efficiently during implementation.
- For ongoing provisioning of new users, you need to work setting up their Global ID as part of your process. There are some tools to help you identify users that are missing a Global ID
 - Special Search: StudentGlobalID
 - Find missing student Global IDs
StudentGlobalID=
 - Query - the following query can help you identify students who have an email address, but whose Global ID is missing or doesn't match their email address. This would identify new students and students whose email address may have changed but the change wasn't applied to the Global ID.

```
SELECT
    students.dcid AS studentsdcid,
    students.student_number,
    students.lastfirst,
    students.grade_level,
    schools.abbreviation AS school,
    emailaddress.emailaddress,
    students.student_allowwebaccess,
    pcas_externalaccountmap.openiduseraccountid AS idp_global_id
FROM
    students
    JOIN schools ON students.schoolid = schools.school_number
    LEFT JOIN accesstudent ON students.dcid = accesstudent.studentsdcid
    LEFT JOIN pcas_externalaccountmap ON accesstudent.accountidentifier =
pcas_externalaccountmap.pcas_accounttoken
    LEFT JOIN personemailaddressassoc ON students.person_id = personemailaddressassoc.personid
    LEFT JOIN emailaddress ON personemailaddressassoc.emailaddressid = emailaddress.emailaddressid
WHERE
    students.enroll_status IN (0,-1)
    AND emailaddress.emailaddress IS NOT NULL
    AND LOWER(nvl(pcas_externalaccountmap.openiduseraccountid,'No IDP')) <>
LOWER(emailaddress.emailaddress)
ORDER BY
    students.lastfirst
```