Microsoft Azure AD SSO Integration with Kurzweil 3000

Last Edited: 3/17/2022

Microsoft Azure AD SSO ("Sign In with Microsoft") offers a range of benefits to Kurzweil 3000 Site or District Web License customers that make use of a Microsoft Azure AD Tenant.

Prerequisites for Microsoft SSO

- Be a Kurzweil 3000 Site or District Web License Subscription customer **[Required]**
- Use a Microsoft Azure AD Tenant **[Required]**
- All users have unique Microsoft Azure AD User Principal Names **[Required]**
- Azure AD Premium P1 subscription (or greater) **[Recommended]**
- Teachers and Students configured in different Azure AD user groups **[Recommended]**

Benefits of Microsoft SSO with Recommended Configuration

- Users can sign into the Kurzweil 3000 tools using their Microsoft credentials
- Users can quickly create their own account tied to their Microsoft credentials
- Teacher and Student initial role designation based upon Azure AD user group
- No roster upload requirements to create users

Interested in Microsoft SSO?

Please send an email to Kurzweil3000Roster@kurzweiledu.com containing answers to the below questions. Please note that we must receive confirmation from your Kurzweil 3000 Top Level Coordinator account before proceeding with implementation.

- What is your Kurzweil 3000 Top Level Coordinator username?
- What Microsoft Azure AD User Principal Name domain/subdomain do your teachers use?
- What Microsoft Azure AD User Principal Name domain/subdomain do your students use?
- Are your teachers and students configured in different Azure AD user groups?
- Do you have an Azure AD Premium P1 subscription or greater?
- If you have existing user accounts, do we have permission to proceed with user deletion to allow for a streamlined SSO integration? [please review 'Integrating SSO with Existing Kurzweil 3000 Users']

Integrating SSO with Existing Kurzweil 3000 Users

If you have existing Kurzweil 3000 users, we'll need to ensure you do not experience issues with duplicate users, or challenges accessing content from these accounts. The most straightforward approach for this is to delete your existing users, except for your Top Level Coordinator. This will ensure all your users using SSO will be associated with the proper Kurzweil 3000 account.

If you have existing users, outside of your Top Level Coordinator, that wish to retain documents they've stored in the Universal Library, they have a couple options:

A. Your Top Level Coordinator account can copy the documents the users wish to retain, into Universal Library folders under the Top Level Coordinator's Private folder. Then copy those documents to the new accounts when they have access.

B. The user can use the 'Download' option under the 'Copy' menu in the Universal Library to save a local copy of the documents they wish to retain. Then upload the documents to their new account when they have access.

If you feel strongly that you have users needing to retain their current accounts, please let us know and we can review the current state of your users. It is possible that you will need to complete additional manual user management to get your existing users aligned with your SSO integration. This can substantially increase the time until your SSO integration is completed.

Microsoft SSO Role Assignment

Kurzweil 3000 has two user roles: teacher and student. You can provide this role information using one of the methods outlined below:

I. Using Azure AD Premium P1 (or greater) with teacher and student user groups **[Recommended]**

Only an Azure AD Premium P1 subscription, or greater, will allow for the assignment of Azure AD user groups to user roles within an application. During configuration of the Kurzweil 3000 Enterprise Application within your Azure AD Tenant, you'll be able to assign your Azure AD user groups to teacher or student roles. It's important that this occurs prior to user provisioning, as this will not change the roles of existing accounts within your Kurzweil 3000 Subscription. [see 'Assigning User Groups to Application Roles']

II. Using different Azure AD User Principal Name domains for teachers/students **[Recommended]**

If you have an implementation where your teachers and students have different User Principal Name domains within your Azure AD Tenant, it can greatly simplify role assignment. Just let us know the User Principal Name domain for both your teachers and students, and when a user attempts to login with the given domain, they'll be automatically provisioned an account with the corresponding user role.

III. Unable to assign user groups to app roles and the same UPN domain for teachers/students

If your Azure AD implementation does not allow for user group assignment to application roles, and you use the same User Principal Name domain for both your teachers and students,

Kurzweil 3000 will be unable to automatically determine the appropriate user role for your users.

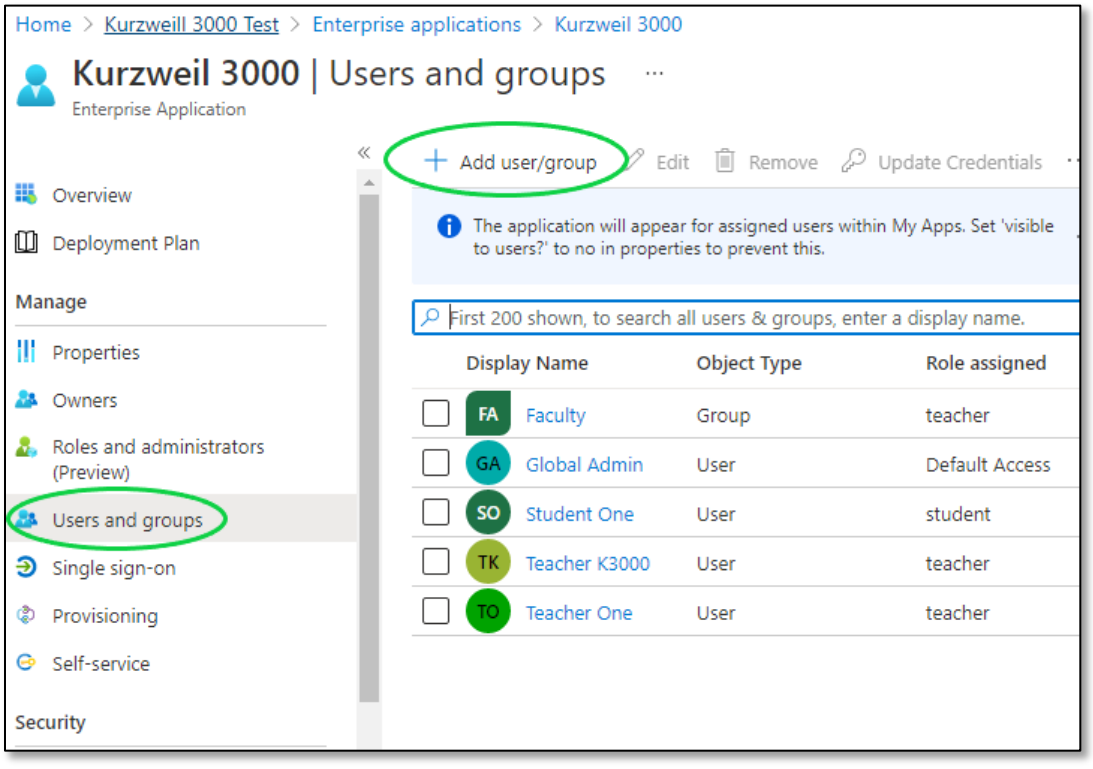
In this scenario:

- Any account that gets created through Microsoft SSO will be assigned the 'student' role. This is the lowest level role available in Kurzweil 3000.
- Any existing Kurzweil 3000 account with Teacher or Top Level Coordinator role access will be able to login to kurzweil3000.com to manually modify user roles to convert students to teachers as needed.

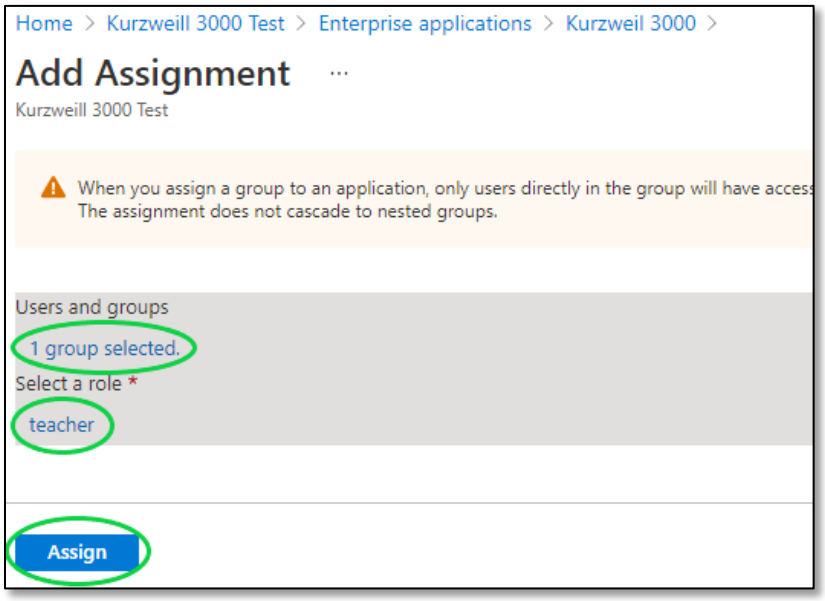
Assigning User Groups to Application Roles

Do you have your faculty and students in separate Azure AD User Groups and do you have at least an Azure AD Premium P1 subscription? If so, you can assign groups to the appropriate role in the application using the steps below:

1. Login to your Azure Portal using your Admin account: https://portal.azure.com/
2. Go to Azure Active Directory > Enterprise Applications
3. Search for Kurzweil 3000 (App ID: 081ba643-6a85-4924-8f06-d36740e88d00) and click on it. If Kurzweil 3000 is not listed, a user from your Azure AD tenant may not yet have attempted to login to kurzweil3000.com using the 'Sign In with Microsoft' button. To get it to appear, attempt to login to kurzweil3000.com using the 'Sign In with Microsoft' button, entering your User Principal Name.
4. Go to Users and Groups
5. Choose Add User/Group at the top

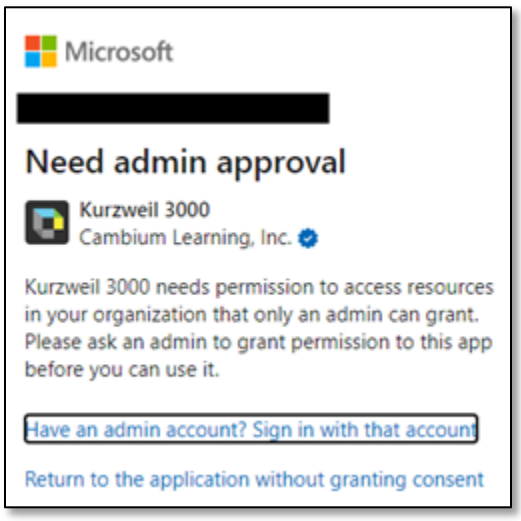


6. Add the faculty/teacher group(s)
7. Select the 'teacher' role (there is no need to assign groups to the ‘student’ role as any user without the ‘teacher’ role will receive the ‘student’ role)
8. Choose 'Assign'



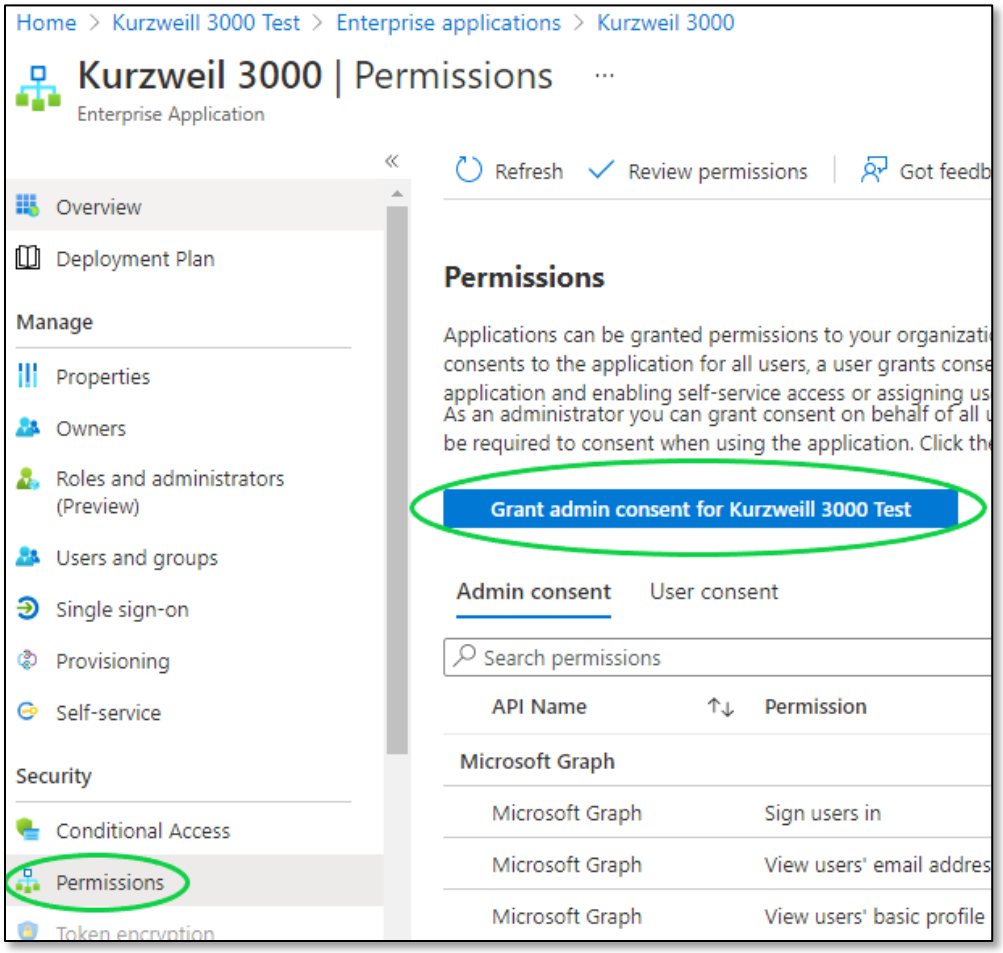
Managing Microsoft Azure AD Application Permissions

An Azure AD Tenant needs to give users Admin consent to access the Kurzweil 3000 application. If a user has not received access, when they attempt to sign into kurzweil3000.com using the ‘Sign In with Microsoft’ button, they will get an error similar to the one below:



The most straightforward way to allow permission is through the steps below which are also covered in the Microsoft Azure AD documentation here: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent

1. Login to your Azure Portal using your Admin account: https://portal.azure.com/
2. Go to Azure Active Directory > Enterprise Applications
3. Search for Kurzweil 3000 (App ID: 081ba643-6a85-4924-8f06-d36740e88d00) and click on it. If Kurzweil 3000 is not listed, a user from your Azure AD tenant may not yet have attempted to login to kurzweil3000.com using the 'Sign In with Microsoft' button. To get it to appear, attempt to login to kurzweil3000.com using the 'Sign In with Microsoft' button, entering your User Principal Name.
4. Go to Permissions
5. Select the 'Grant admin consent for [Azure AD Name]' button, which will allow access for all users within your Tenant. If you'd prefer to only allow permissions for specific groups or individual users, please refer to Microsoft's documentation.

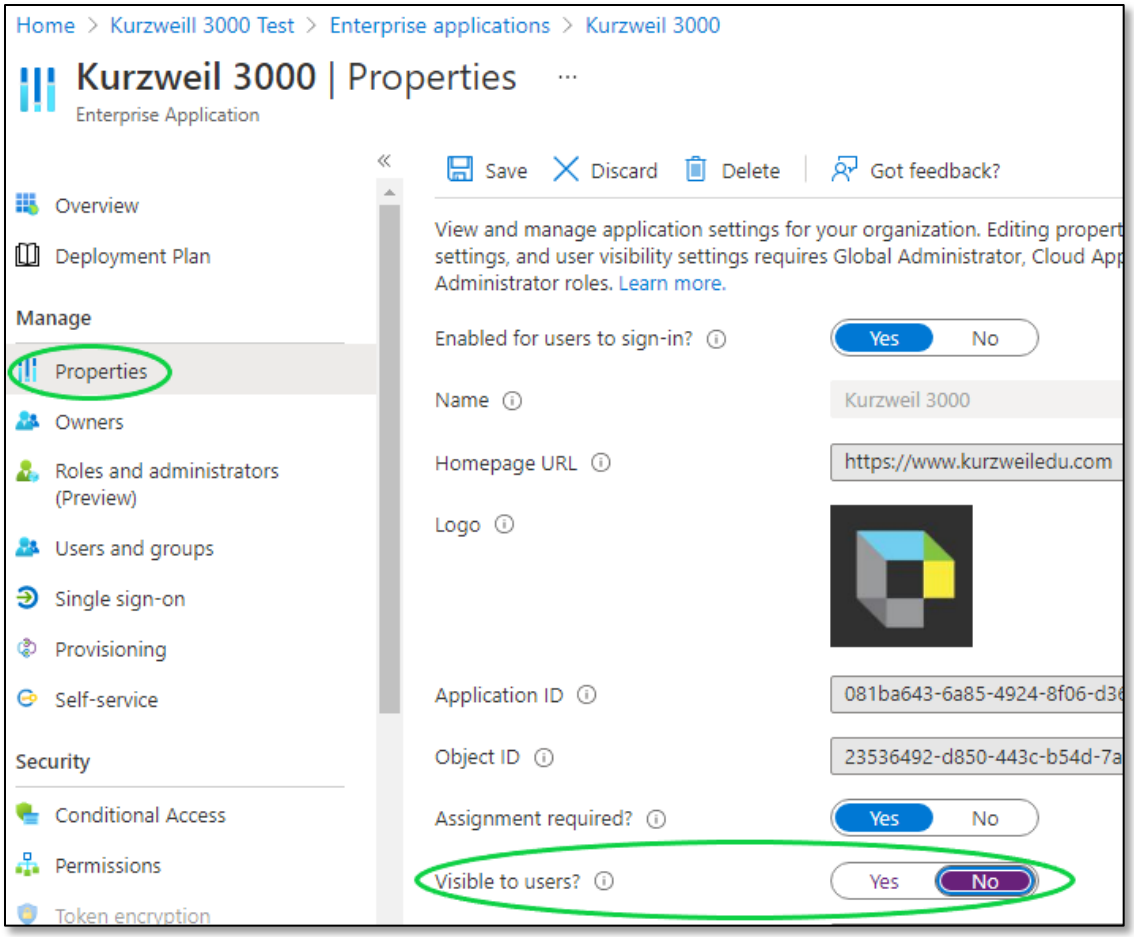


Kurzweil 3000 Application Visibility within Office 365

By default, an Azure AD Tenant will allow all Enterprise Applications to be visible to users within the Office 365 environment. Given that Kurzweil 3000 is commonly used as a more directed tool, you may wish to hide it in this location.

If you're concerned about visibility of the Kurzweil 3000 application, you can make the app invisible to your users. Users will still be able to navigate to kurzweil3000.com and sign in with their Microsoft credentials, but they will not see the Kurzweil 3000 app listed in Office 365:

1. Login to your Azure Portal using your Admin account: https://portal.azure.com/
2. Go to Azure Active Directory > Enterprise Applications
3. Search for Kurzweil 3000 (App ID: 081ba643-6a85-4924-8f06-d36740e88d00) and click on it. If Kurzweil 3000 is not listed, a user from your Azure AD tenant may not yet have attempted to login to kurzweil3000.com using the 'Sign In with Microsoft' button. To get it to appear, attempt to login to kurzweil3000.com using the 'Sign In with Microsoft' button, entering your User Principal Name.
4. Go to Properties
5. Set 'Visible to users?' to 'No'
6. Choose 'Save'



Completed Microsoft SSO Integration

Once we have completed the integration of your Kurzweil 3000 Subscription with Microsoft SSO, your existing users, and any new user that needs access to Kurzweil 3000, will be able to login using their Microsoft credentials through the 'Sign In with Microsoft' button on

https://www.kurzweil3000.com/KLogin.php or directly through https://www.kurzweil3000.com/MicrosoftLoginRedirect.php

The first time a user attempts to sign into Kurzweil 3000 using their Microsoft credentials, they will be provisioned a Kurzweil 3000 user account with an assigned role based on the implementation type you're using [see 'Microsoft SSO Role Assignment'].

If they receive a permissions prompt, their account has not been provided admin consent within your Azure AD Tenant [see 'Managing Microsoft Azure AD Application Permissions'].

Enable Microsoft Button for Kurzweil 3000 Windows

By default, the Kurzweil 3000 Web License Subscription Windows installed client will not display a button allowing Microsoft SSO. This button can be enabled by passing a few registry changes.

1. Ensure you have at least Kurzweil 3000 v20.10 installed on the machine. You can download the latest patch for your version of Kurzweil 3000 here: https://www.kurzweiledu.com/products/software-updates.html
2. Create/Deploy a registry script that contains the below modifications:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KESI\Kurzweil 3000\WebLic]

"ShowSsoOptions"="1"

"ShowGoogleSso"="0"

"ShowClassLinkSso"="0"

"ShowMicrosoftSso"="1"

"SsoTimeout"="45"

[HKEY_LOCAL_MACHINE\SOFTWARE\KESI\Kurzweil 3000\WebLic]

"ShowSsoOptions"="1"

"ShowGoogleSso"="0"

"ShowClassLinkSso"="0"

"ShowMicrosoftSso"="1"

"SsoTimeout"="45"
```

Enable Microsoft Button for Kurzweil 3000 Mac

By default, the Kurzweil 3000 Web License Subscription Mac installed client will not display a button allowing Microsoft SSO. This button can be enabled by running/deploying a separate utility.

1. Ensure you have at least Kurzweil 3000 v20.10 installed on the machine. You can download the latest patch for your version of Kurzweil 3000 here: https://www.kurzweiledu.com/products/software-updates.html

2. Run/Deploy the 'turnOnSSOMicrosoft' app found in the compressed archive here: https://support.kurzweiledu.com/index.php?pg=file&from=2&id=319

Frequently Asked Questions

What email address should my Kurzweil 3000 Top Level Coordinator account use for Microsoft SSO?

We do not tie a Kurzweil 3000 Top Level Coordinator account to a Microsoft account. This is to prevent access issues should the account need to be provided to another individual within the organization. You'll need to use your Kurzweil 3000 username and password to login as your Top Level Coordinator account.

How do you determine which users are teachers, and which users are students?

We support several different SSO integration methods with Microsoft Azure AD. How users are assigned roles within Kurzweil 3000 will be determined based on which integration method your organization uses [see 'Microsoft SSO Role Assignment'].

Once a user has been provisioned a Kurzweil 3000 account through your Microsoft Azure AD Tenant, the account's role cannot be modified through Azure AD Tenant modifications (i.e.: changing the assigned role within your Azure AD Tenant). The only way to modify the account's role would be for a teacher or Top Level Coordinator account to login to kurzweil3000.com and manage the account manually.

What permissions do you request from users to utilize Microsoft SSO?

We require the following Microsoft permissions for each account utilizing Microsoft SSO:

- Sign users in
- View users' email address
- View users' basic profile
- Maintain access to data you have given it access to
- Sign in and read user profile
- Read all users' basic profiles
- Read items in all site collections
- Read users' view of the roster
- Read a limited subset of users' view of the roster
- Read users' class assignments without grades
- Read and write users' class assignments without grades

Why are my users receiving an error message when they use the 'Sign In with Microsoft' button?

If your users receive the error, "Your email address needs to be a school email address that has been authorized for access to Kurzweil 3000 via Microsoft. Please contact your teacher or school administrator for help getting this configured", please review the troubleshooting information here: https://support.cambiumtech.com/index.php?pg=kb.page&id=1879

If we configure Microsoft SSO, can users still login with their Kurzweil 3000 credentials?

Yes. Users will have the option to sign in using either their associated Microsoft credentials through the 'Sign In with Microsoft' buttons, or by using their Kurzweil 3000 username and password in the username/password prompts.

What Kurzweil 3000 tools can I access using my Microsoft credentials?

Once your subscription is configured to make use of Microsoft SSO, you'll be able to use your Microsoft credentials to access the following Kurzweil 3000 tools:

- kurzweil3000.com
- Kurzweil 3000 Read the Web extension
- Kurzweil 3000 Windows (See 'Enable Microsoft Button for Kurzweil 3000 Windows')
- Kurzweil 3000 Mac (See 'Enable Microsoft Button for Kurzweil 3000 Mac')

Will Microsoft SSO delete users from our Kurzweil 3000 subscription when they should no longer have access?

No. Microsoft integration will not delete any users from your Kurzweil 3000 subscription. If you need to delete a user, you can do so through the kurzweil3000.com interface (please see page 16 of the document here: https://www.kurzweiledu.com/files/pdf/kurzweil3000com/user_and_license_management.pdf) If you need to delete users in bulk, you can make use of our rostering service to upload a CSV containing all of your desired users. (please review the document here: https://support.cambiumtech.com/index.php?pg=file&from=2&id=301).

When a user is created through Microsoft SSO, what will be entered as their school/organization?

Microsoft does not provide school/organization association during its authentication. Any user created through Microsoft SSO will have the same school/organization association as the Top Level Coordinator account in your subscription. You can view/change the association by logging into kurzweil3000.com as your Top Level Coordinator account, then going to My Account > Profile, and viewing the 'School/Organization Selector'. The school/organization entered here will be used for all newly created Microsoft SSO users.

Can we use Kurzweil 3000's 'Offline Mode' while also making use of Single Sign On?

Single Sign On requires internet access to verify the secure trust relationship between Kurzweil 3000 and your Single Sign On provider. You won't be able to use Offline Mode in conjunction with Single Sign On. If you'd like to use Offline Mode, you'd need to have your users login with their assigned Kurzweil 3000 credentials, instead of their SSO credentials.