MySchoolBucks Single Sign On

	Introduction
1	This document is to serve as a reference for the values that can to be expressed for the different MySchoolBucks (MSB) user roles. There are a number of roles that support optional expression of department, school, and store designations but are not typical usage.
2	Recommendations within this document are made with the intent of doing all of the possible setup within the integration period; allowing all account maintenance to be done on the district side as needed. For example, creating groups to all MySchoolBucks roles and using those to assign and maintain access from the district side will reduce or eliminate the need for configuration changes within MSB or our Single Sign On application to reflect role changes with your organization.
3	MySchoolBucks Developer Services team can be contacted regarding technical questions at MSBDeveloperServicesTeam@e-hps.com. Administrative or product questions should be sent to your Heartland School Solutions account manager.
	Overview and Business Rules
1	Role mapping from Identity Provider (IDP) on the district side to MySchoolBucks will take place in a Red Hat SSO middleware appliance. Account attributes including groups, names, email, and other defined attributes can be used to map the district settings into MSB. (See 'Claim Mapping' tab for details.)
2	MSB will operate on the concept of least privilege, so administrative accounts with multiple group memberships will be granted the lowest role that appears in their claim. Consider this principle as group assignments are made; putting "All Users" into a default "Parent" role in MSB will eliminate any elevated rights for administrative users.
3	MSB will assign limiting resources (department, school, store) at login, so any previous settings will be replaced. This will include the implied removal of filtering if an account had previously been assigned a limit if no assignment appears in a subsequent claim during login. If a required value is missing, the login will fail.
4	MSB does not support parent and admin login from the same IDP account. Once an account is created as parent or admin with an IDP login, it cannot be used in another context.

5	If parent role IDP user has never used MySchoolBucks before, MSB will create a native user account and link the IDP login to it. If user leaves the school district, the account can continue to be accessed with the MSB login.
6	If a parent role IDP user has an existing MySchoolBucks account, MSB will allow account linking to the IDP login for it. If user leaves the school district, the account can continue to be accessed with the MSB login.
7	Admin role IDP users will have MSB accounts created at first login, but the password and security questions will not be collected and the account cannot be accessed with an MSB login. This account can only be accessed with the IDP login so the district can control its permissions without forcably removing account rights in both systems.
Recommendations	
1	As soon as possible at the beginning of the process, send the MSB Developer Services team your federation URL so it can be added to our Proxy whitelist and added to our SSO appliance.
2	The MSB Developer Services team will send a URL for each of our integration environments to establish a relying party trust between your IDP and our SSO. You will need to apply this information to your services before we can initiate testing.
3	The Dev Services team strongly encourages use of a test IDP, if available. Production IDP can also be used, provided that there are test accounts and/or test groups that won't permit any access to production users until we have certified all roles.
4	The MSB team also strongly encourages test accounts to be created for each role and shared with us so we can test independent of the availability of your development resources. If this isn't possible, we will require scheduling of frequent developer integration sessions where your team will initiate logins so we can retrieve the claim details, complete setup, and do MSB role verification.
5	Create groups internal to your IDP that controls MySchoolBucks role mapping. This is commonly used to control permissions with internal applications that support Active Directory login. Your users or groups would be assigned to MSB_DistrictAdmin, MSB_StoreAdmin, MSB_Teacher, etc. (for example) and these would be the collections we map to our internal accounts.

6	Once the internal role mapping groups are created, communicate the roles to the MSB Developer Services team to begin the claim mapping process. Include the SID and group name for all roles.
7	Include the SID value of all group memberships in the ADFS claims to the MSB SSO server. Our application will only be able to activate on known, defined values, so all other groups are ignored as undefined resources for our service.
8	When creating groups for MSB role mapping, include all roles so the claim mapping can be created at initial integration. Any groups that the district does not intend to use at the outset of SSO logins can be internally disabled within the IDP.

MySchoolBucks Single Sign On

MSB Role	Email	First Name	Last Name	Security Groups
Parent	Required. Will prompt user if there are new changes from IDP to MSB.	Optional (will collect at login if absent). Will prompt user if there are new changes from IDP to MSB.	Optional (will collect at login if absent). Will prompt user if there are new changes from IDP to MSB.	Required, expressed as SID values (mapping to roles will be supported by HSS when onboarding SSO)
* ALL ADMIN ROLES *	Required. Will update to IDP value on every login.	Optional (will collect at login if absent). Will update to IDP value on every login.	Optional (will collect at login if absent). Will update to IDP value on every login.	Required, expressed as SID values (mapping to roles will be supported by HSS when onboarding SSO)

MSB Role	Department	School	Store
Description of effect this setting has for the eligible roles.	Used to filter reporting results via eTransfer or Admin reports.	Used to limit scope of configuration and sales of items in store roles. Used to filter reporting results via eTransfer or Admin reports.	Used to limit scope of configuration and sales of items in store roles. Used to filter reporting via admin reports.
Parent	Ignored	Ignored	Ignored
Teacher	Optional	Optional	Optional
Store Clerk	Optional	Optional	Required
Store Admin	Optional	Optional	Required
Report Admin	Optional	Optional	Optional
Business Admin	Optional	Optional	Optional
School Admin	Optional	Required	Optional
District Accountant	Optional	Optional	Optional
District Admin	Optional	Optional	Optional
Department Admin	Required	Optional	Optional

MySchoolBucks Single Sign On

First IDP Login

Feature	Admin role	Parent role new account	Parent role with MSB login
Can log in from external portal	Yes	Yes	Yes
Can log in from MSB	No	No	No (account not tied to IDP yet)
Checks if IDP account is mapped to MSB	Yes	Yes	Yes
Checks if IDP role matches MSB	Yes	No	Yes
Ask to link existing account	No	Yes	Yes
MSB login to link account	N/A	No OR on failed login OR on non-parent login	Yes
Update user to user info from IDP	Yes	Yes	Ask
Create new user	Yes	Yes	No
Request account details (security questions, etc.)	No	Yes	Only if missing
Request MSB password	No	Yes	No

MySchoolBucks Single Sign On

Return IDP Logins

Feature	Admin role	Parent role
Can log in from external portal	Yes	Yes
Can log in from MSB	Yes	Yes
Checks if IDP account is mapped to MSB	Yes	Yes
Checks if IDP role matches MSB	Yes	Yes (won't allow IDP parent to access MSB admin account)
Ask to link existing account	No	No
MSB login to link account	N/A	No
Update user to user info from IDP	Yes	Ask
Create new user	Yes	No
Request account details (security questions, etc.)	No	Only if missing
Request MSB password	No	No