

Requirements Analysis

Smarter Balanced Assessment Consortium Test Delivery System

Component: Administration and Registration Tools

Purpose: Smarter Balanced Task Order 15, Improved Security and Usability

Revision History

Revision Description		Date
First Draft	Rami Levy	August 20, 2015
1.0. Add accommodations format update for compatibility with Task Order 10, and update Student Group import/export changes.	Rami Levy	October 27, 2015
1.1. Added requirement section in 3.6 about allowing coordinator to SYNC, LOCK, and UNLOCK. Added risk (Section 4) indicating possible downside.	Rami Levy	November 16, 2015
1.2. Add clarification to requirements 3.5, 3.6, 3.7 about when the user changes take effect.	Rami Levy	January 4, 2016
1.3. Update Figure 8 with more accurate mockup. Add Figure 8 closeup view. Update section 3.9.3 to include export of ExplicitEligibility.	Rami Levy	February 23, 2016

Contents

1	Background	4
1.1	Problem Description	4
1.2	Proposed Solution.....	4
2	Requirements	5
3	Description of Changes.....	9
3.1	Requirement 1: View Users with Roles Within Jurisdiction	9
3.2	Requirement 2: View Roles Within Jurisdiction	9
3.3	Requirement 3: Reset Password	9
3.4	Requirement 4: Send Initiator Info On Reset Password	9
3.5	Requirement 5: Delete User When Last Role Deleted	10
3.6	Requirement 6: Restrict Editing Users Partially Within Jurisdiction	10
3.7	Requirement 7: Self-Service User Profile	11
3.8	Requirement 8: Self-Service Change Password	12
3.9	Requirement 9: Harmonize Export and Import File Formats	13
3.9.1	Changes Applicable to All Exports	13
3.9.2	State, District, Institution, User, Group of Institutions, Group of Districts, Group of States	13
3.9.3	Students.....	16
3.9.4	Student Groups.....	18
3.9.5	Accommodations	18
4	Risks.....	18

Figures

Figure 1: Option B: Allow user to cancel out.....	9
Figure 2: Immutable User Info Screen.....	11
Figure 3: User Menu	11
Figure 4: User Profile Mockup	12
Figure 5: Delete Role Warning	13

Figure 6: Delete Last Role Warning	13
Figure 7: New Student File Export Pane	17
Figure 8: Student File Export choices	17

Tables

Table 1: Analysis of Task Order 15 Requirements	7
---	---

1 Background

Among other functions, the Smarter Balanced Administration and Registration Tools (ART) system allows for the registration and management of users at various levels of jurisdiction. ART's security model is based on the "if you see it, you can edit it" paradigm. While this prevents the editing of users outside of one's jurisdiction, it also reduces the usability in situations where users have roles in multiple jurisdictions.

1.1 Problem Description

When a user has roles aligned to more than one entity, only coordinators which are hierarchically above all of the user's roles can see that particular user. This has a number of manifestations.

- When a coordinator attempts to add a user and grant a role within their district or school, and that user account already exists with one or more roles elsewhere, the system succeeds and grants the user the new role. However, the user and new role remain invisible to the coordinator so it appears to have failed. Coordinators perceive this as a bug.
- The initial provisioning created all users at the state level which is higher than the coordinator level. Thus, there are thousands of users that remain invisible after they have roles added at the district or school levels. For a temporary remedy, we have a nightly batch process that removes the state-level DL_EndUser role for any users that are found to have another DL_EndUser role at a school or district. This makes those accounts appear the day after a coordinator adds them.

1.2 Proposed Solution

Smarter Balanced Task Order 15 commissions ART software development to make changes that improve usability of ART while preserving security.

- Security must be preserved. The existing behavior is to preserve security. Presently any coordinator (State, District, or School) can change the email address of any user they can see and force a password reset. If visibility were granted to all users with roles in their jurisdiction and access rights were unchanged, a district coordinator could grant the DL_EndUser role to someone higher up in the chain, such as a state coordinator, change that coordinator's email address, perform a password reset, and they would be able to hijack any user's account.
- Behavior should not include anything that is perceived by a user or coordinator as a bug.
- Ability to reset passwords and update email addresses must be preserved.
- Harmonizing of ART export and import formats.

2 Requirements

Task Order 15 proposed changes received via email on July 30, 2015 from Smarter Balanced are as follows:

1. All users with roles that are within the domain of a Coordinator (Client Coordinator, State Coordinator, District Coordinator, or School Coordinator) should be visible to that coordinator when searching or looking up.
2. Only roles that are within a Coordinator's domain(s) shall appear to that coordinator. Coordinators should NOT be able to view, edit, or remove roles that are outside their domain.
3. Coordinators should be able to initiate a password reset for any user within their domain. The confirmation window for the password reset should inform the coordinator that their name will be sent to the user in the password reset message informing the user who initiated the reset process. (This is to reduce abuse of the feature.)
4. Password reset messages should include the name of the coordinator who initiated the reset.
5. When the last role for a user is removed, that user account should be deleted.
6. Coordinators should NOT be able to change the name, email address or phone number for a user if they have roles outside the coordinator's domain. This limitation applies both to the UI and to bulk uploads.
7. Users should be able to access their own information in ART. The information displayed should include the following:
 - Name, Email Address, Phone Number, All Assigned Roles
8. Users should be able to edit their own information in ART
 - Change Password, Change Email Address, Change Name, Change Phone Number
 - Delete Assigned Roles (but not add roles). A confirmation screen should warn the user that when a role is deleted they will have to contact a coordinator to restore the role. Confirmation should require that the user type something such as the name of the role to confirm this action.
9. Modify the export format for Institutions, Students, and Users to match the import formats for these entities.

The following table analyzes the requirements and provides a description of the technical approach towards addressing the requirement. This includes changes based on further discussions with Smarter Balanced.

Req. No.	Requirement	Technical Approach
1	All users with roles that are within the domain of a Coordinator (Client Coordinator, State Coordinator, District Coordinator, or School Coordinator) should be visible to that coordinator when searching or looking up.	<ul style="list-style-type: none"> Functions handling jurisdictional searching shall return results of users even if those users have roles outside the jurisdiction of the logged-in user. Function of adding a new user whose email address matches an existing user changes to allow this addition by simply adding the new roles to the existing user's roles but ignoring any changes to user information (name/phone).
2	Only roles that are within a Coordinator's domain(s) shall appear to that coordinator. Coordinators should NOT be able to view, edit, or remove roles that are outside their domain. Coordinators shall be able to view, edit, and remove user roles that are within their jurisdiction.	Functions handling display of user roles only show roles within the jurisdiction of the logged-in user.
3	Coordinators should be able to initiate a password reset for any user within their domain. The confirmation window for the password reset should inform the coordinator that their name will be sent to the user in the password reset message informing the user who initiated the reset process. (This is to reduce abuse of the feature.)	User interface changes to add a pop-up confirmation window informing logged-in user that their name will be included in the password reset message to the user.
4	Password reset messages should include the name of the coordinator who initiated the reset.	Add optional node in the provisioning XML that contains the text of the message to be sent along with the existing password reset notice. This involves modification of the provisioning script on the OpenDJ server, as well as the XML generation function in ART.
5	When the last role for a user is removed, that user account should be deleted.	This was implemented as part of SB-1259
6	Coordinators should NOT be able to change the name, email address or phone number for a user if they have roles outside the coordinator's domain. This limitation applies both to the UI and to bulk uploads.	Functions which display the user information data should make the data immutable on the screen in the case where the displayed user has roles outside the logged-in user's jurisdiction. The UI will provide an informational notice that the user may change this info by editing their profile, but the coordinator/logged-in user cannot change it.
7	Users should be able to access their own information in ART. The information displayed should include the following: Name Email Address Phone Number All Assigned Roles	A new "self-service" function will be available that will mimic the Create/Modify Users page. This function will be accessible from the "Logged in" text at the top right of all ART pages.

Smarter Balanced Test Delivery System High Level Requirements – Task Order 15

Req. No.	Requirement	Technical Approach
8	<p>Users should be able to edit their own information in ART: Change Password Change Email Address Change Name Change Phone Number Delete Assigned Roles (but not add roles). A confirmation screen should warn the user that when a role is deleted they will have to contact a coordinator to restore the role. Confirmation should require that the user type something such as the name of the role to confirm this action.</p>	<ul style="list-style-type: none"> • A new function "self-service" function will be available that will mimic the Create/Modify Users page, with limited editing functionality (same as above). This function will be accessible from the "Logged in" text at the top right of all ART pages. This function will prevent the addition of new roles, modification of existing roles, but will allow deletion of existing roles. • Confirmation screen will show when deleting a role, requiring the user to type the name of the role to confirm deletion. Comparison will be case-insensitive. User will be allowed to continue or cancel. When the user's last role is about to be deleted by the user, a pop-up message will show, warning that this will permanently delete their account from ART, and allowing the user to continue or cancel.
9	<p>Modify the export format for Institutions, Students, and Users to match the import formats for these entities.</p>	<ul style="list-style-type: none"> • Generally, all export formats and many import formats will require modification in order to harmonize the exports with the imports. • Export column names will match to the import names. • In cases where organizational IDs and Names don't exist in both formats, this will be updated (and be made optional/ignored by the imports). This means that the column must exist but the data is optional. • A Delete column will be provided on all exports as required by the imports. • New functionality will be added to provide an export of the student explicit eligibility collection. • A four-radio-button group for selecting student export type (student+accommodations, student, accommodations, explicit eligibility) will be used to allow selection of the appropriate student information export. • An informational message will be provided regarding required-but-ignored columns, in file upload page after selecting entity type. • CSV imports will support for commas within names.

Table 1: Analysis of Task Order 15 Requirements

3 Description of Changes

The following details the changes required in ART:

3.1 Requirement 1: View Users with Roles Within Jurisdiction

All users with roles that are within the domain of a Coordinator (Client Coordinator, State Coordinator, District Coordinator, or School Coordinator) should be visible to that coordinator when searching or looking up.

No changes in user interface from the current implementation of ART. The implementation is described in Table 1.

3.2 Requirement 2: View Roles Within Jurisdiction

Only roles that are within a Coordinator's domain(s) shall appear to that coordinator. Coordinators should NOT be able to view, edit, or remove roles that are outside their domain. Coordinators shall be able to view, edit, and remove user roles that are within their jurisdiction.

No changes in user interface from the current implementation of ART. The implementation is described in Table 1.

3.3 Requirement 3: Reset Password

Coordinators should be able to initiate a password reset for any user within their domain. The confirmation window for the password reset should inform the coordinator that their name will be sent to the user in the password reset message informing the user who initiated the reset process. (This is to reduce abuse of the feature.)

The password reset informational popup would show up *prior* to the transmission of the password reset, allowing the user to cancel his/her actions (see Figure 1).

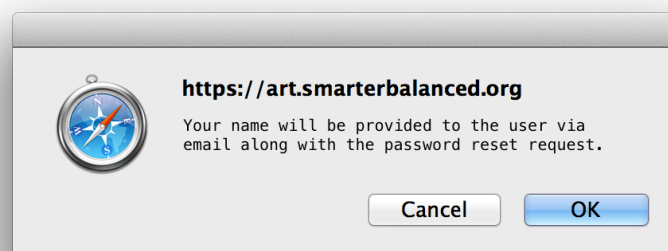


Figure 1: Option B: Allow user to cancel out

3.4 Requirement 4: Send Initiator Info On Reset Password

Password reset messages should include the name of the coordinator who initiated the reset.

Add an optional node in the provisioning XML that contains the text of the message to be sent along with the existing password reset notice. This involves modification of the OpenDJ provisioning script, as well as the XML generation function in ART.

If the current email content is:

Your Smarter Balanced password has been reset. Your temporary password is: DxxUA1!
You are required to change your password the next time you log in.
[Click here](#) to access your Smarter Balanced account now.

And the provisioning XML contained the following additional and optional node:

```
<Message>Your password was reset by John Smith (jsmith@mailinator.com) on Monday, August 17, at 8:50AM ET.</Message>
```

Then the new password reset email should contain:

Your Smarter Balanced password has been reset. Your temporary password is: DxxUA1!
Your password was reset by John Smith (jsmith@mailinator.com) on Monday, August 17, at 8:50AM ET.
You are required to change your password the next time you log in.
[Click here](#) to access your Smarter Balanced account now.

If the <Message> node is blank or missing from the XML, the email message content would remain unchanged.

3.5 Requirement 5: Delete User When Last Role Deleted

When the last role for a user is removed, that user account should be deleted.

This has already been implemented in ART and released April 24, 2015.

NOTE: If the affected user is *not* currently logged in, user deletion only takes effect after the user export frequency time period has elapsed (see Program Management ART parameter `testreg.user.export.frequency.milliseconds`); this is usually two minutes. If the affected user *is* currently logged in, the deletion takes effect only after that user logs out.

3.6 Requirement 6: Restrict Editing Users Partially Within Jurisdiction

Coordinators should NOT be able to change the name, email address or phone number for a user if they have roles outside the coordinator's domain. This limitation applies both to the UI and to bulk uploads.

When a logged-in user views a user with roles outside the logged-in user's domain, the viewed user's name, address, and phone number shall be immutable (see Figure 2).

Coordinator shall be able to SYNC, LOCK, and UNLOCK a user's account, even if they have roles outside the coordinator's domain.

Edit User Information	★ Indicates required field
★ First Name: <input type="text" value="AalborgVolper"/>	★ Last Name: <input type="text" value="Mary"/>
★ Email Address: <input type="text" value="maalborg@wusd.org"/>	Telephone Number: <input type="text"/>
<p>This user has roles outside your jurisdiction, so you cannot edit their names and phone number. Please contact the user (or a higher-level administrator) and have them change this user's information.</p>	
Role Associations	

Figure 2: Immutable User Info Screen

NOTE: If the affected user is *not* currently logged in, these changes only takes effect after the user export frequency time period has elapsed (see Program Management ART parameter `testreg.user.export.frequency.milliseconds`); this is usually two minutes. If the affected user *is* currently logged in, the changes take effect only after that user logs out.

3.7 Requirement 7: Self-Service User Profile

Users should be able to access their own information in ART. The information displayed should include the following: Name, Email Address, Phone Number, All Assigned Roles

In order for users without ART roles to be able to edit their profiles in ART, their roles must contain an additional (new) permission that will allow *Edit Profile* access. The following new sub-requirements follow:

- A user with a role that includes *Edit Profile* permission will be allowed to see the **Edit Profile** menu selection.
- A user without a role having the *Edit Profile* permission will not see the **Edit Profile** selection.
- A user with only the *Edit Profile* permission will be directed immediately to their profile page.
- This profile page will have a directly-accessible URL as well (e.g. `/user/profile`).
- This profile page should be accessed via their *Name* menu, which would serve as a menu in the same way the other menus work (*Settings* and *Resources*) (see Figure 3).
- This menu's options shall be **Edit Profile** and **Logout** link (see Figure 3).

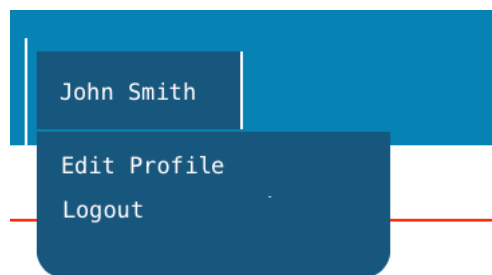


Figure 3: User Menu

NOTE: These changes take effect only after the user logs out.

3.8 Requirement 8: Self-Service Change Password

Users should be able to edit their own information in ART: Change Password

Change Email Address, Change Name, Change Phone Number, Delete Assigned Roles (but not add roles). A confirmation screen should warn the user that when a role is deleted they will have to contact a coordinator to restore the role. Confirmation should require that the user type something such as the name of the role to confirm this action.

As in the previous requirement, once the user selects **Edit Profile**, they will shown a screen similar to Create/Modify User, but with new restrictions (see Figure 4):

- User can delete roles but not add new roles or edit existing roles;
- User can reset their own password but not Sync, Lock, or Unlock their account.

Administration and Registration Tools

Settings Resources Logged in as: Rami Levy Admin Tenant: CLIENT - 1000

* Warning: You have unsaved changes

Edit User Information

* Indicates required field

* First Name: AalborgVolper * Last Name: Mary

* Email Address: maalborg@wusd.org Telephone Number:

Role Associations

* Role	* Responsible Entity Type	* Associated Entity Id	State
School Coordinator	INSTITUTION	01212360000000 - North County Consortium ...	CA
DL_EndUser	INSTITUTION	01212360000000 - North County Consortium ...	CA

✓ Save ✕ Cancel

User Actions

✓ Reset Password

Figure 4: User Profile Mockup

After a user attempts to delete one of their roles, a confirmation pop-up should appear, with appropriate warnings.

- Delete a role that is not the last role of the user:

- "WARNING: If you delete this role, you must contact your coordinator to restore it. To confirm, please type DELETE here:" (see Figure 5).

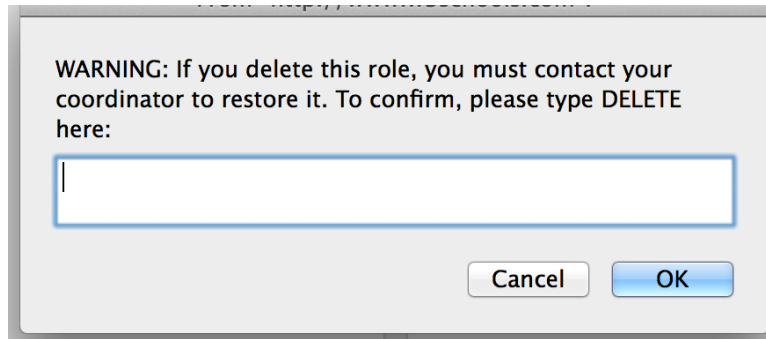


Figure 5: Delete Role Warning

- Delete a role that is the last role of the user (see Figure 6):
 - "WARNING: If you delete this role, your account will be permanently deleted from ART. To confirm, please type DELETE here:"

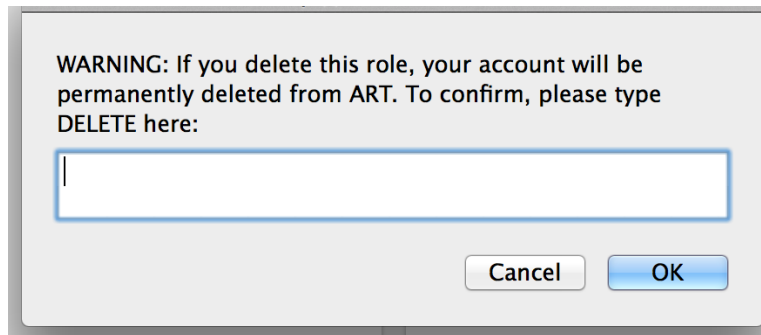


Figure 6: Delete Last Role Warning

3.9 Requirement 9: Harmonize Export and Import File Formats

Modify the export format for Institutions, Students, and Users to match the import formats for these entities.

This requirement implies changes to both the upload file format and the export formats. A summary of these changes is below, followed by a detailed description of the changes to the upload formats.

3.9.1 Changes Applicable to All Exports

- Remove spaces from column headers
- Add *Delete* column as a last column

3.9.2 State, District, Institution, User, Group of Institutions, Group of Districts, Group of States

- Add column *ParentEntityName* in **import** format (validation and templates).
- Add column *ParentExternalId* in **export** formats. *ParentExternalId* should immediately precede *ParentEntityName*, and they should be in a same place as in the current version of import or export.
- For Users export, change Email Address to *ElectronicMailAddress*.

3.9.2.1 Group of States

GroupOfStatesIdentifier	GroupOfStatesName	ParentEntityType	ParentExternalId	ParentEntityName	Delete
-------------------------	-------------------	------------------	------------------	------------------	--------

Field Name	Display Name	Reference	Width	Required	Data Element Description	Data Type	Acceptable Values	Definitions	Example
ParentEntityName	N/A	N/A	50	N	A unique number or alphanumeric code assigned to an organization by a school, school system, a state, or other agency or entity.	Alphanumeric/special xsd:token	One or more ASCII characters		Client_name

3.9.2.2 State

StateAbbreviation	StateName	ParentEntityType	ParentExternalId	ParentEntityName	Delete
-------------------	-----------	------------------	------------------	------------------	--------

Field Name	Display Name	Reference	Width	Required	Data Element Description	Data Type	Acceptable Values	Definitions	Example
ParentEntityName	N/A	N/A	50	N	A unique number or alphanumeric code assigned to an organization by a school, school system, a state, or other agency or entity.	Alphanumeric/special xsd:token	One or more ASCII characters		SGroup1

3.9.2.3 Group of Districts

GroupOfDistrictsIdentifier	GroupOfDistrictsName	ParentEntityType	ParentExternalId	ParentEntityName	StateAbbreviation	Delete
----------------------------	----------------------	------------------	------------------	------------------	-------------------	--------

Field Name	Display Name	Reference	Width	Required	Data Element Description	Data Type	Acceptable Values	Definitions	Example
ParentEntityName	N/A	N/A	50	N	A unique number or alphanumeric code assigned to an organization by a school, school system, a state, or other agency or entity.	Alphanumeric/special xsd:token	One or more ASCII characters		Virginia

Smarter Balanced Test Delivery System High Level Requirements – Task Order 15

3.9.2.4 District

LocalEducationAgencyIdentifier	OrganizationName	NCESLEAID	ParentEntityType	ParentExternalId	ParentEntityName	StateAbbreviation	Delete
--------------------------------	------------------	-----------	------------------	------------------	------------------	-------------------	--------

Field Name	Display Name	Reference	Width	Required	Data Element Description	Data Type	Acceptable Values	Definitions	Example
ParentEntityName	N/A	N/A	100	N	A unique number or alphanumeric code assigned to an organization by a school, school system, a state, or other agency or entity.	Alphanumeric/special xsd:token	One or more ASCII characters		DGroup1

3.9.2.5 Group of Institutions

GroupOfInstitutionsIdentifier	GroupOfInstitutionsName	ParentEntityType	ParentExternalId	ParentEntityName	StateAbbreviation	Delete
-------------------------------	-------------------------	------------------	------------------	------------------	-------------------	--------

Field Name	Display Name	Reference	Width	Required	Data Element Description	Data Type	Acceptable Values	Definitions	Example
ParentEntityName	N/A	N/A	100	N	A unique number or alphanumeric code assigned to an organization by a school, school system, a state, or other agency or entity.	Alphanumeric/special xsd:token	One or more ASCII characters		District

3.9.2.6 Institution

InstitutionIdentifier	NameOfInstitution	ParentEntityType	NCESInstitutionId	ParentExternalId	ParentEntityName	StateAbbreviation	Delete
-----------------------	-------------------	------------------	-------------------	------------------	------------------	-------------------	--------

Field Name	Display Name	Reference	Width	Required	Data Element Description	Data Type	Acceptable Values	Definitions	Example
ParentEntityName	N/A	N/A	100	N	A unique number or alphanumeric code assigned to an organization by a school, school system, a state, or other agency or entity.	Alphanumeric/special xsd:token	One or more ASCII characters		IGroup1

3.9.2.7 Users

FirstName	LastOrSurname	ElectronicMailAddress	TelephoneNumber	Role	AssociatedEntityID	ParentEntityName	Level	StateAbbreviation	Delete
-----------	---------------	-----------------------	-----------------	------	--------------------	------------------	-------	-------------------	--------

Field Name	Display Name	Reference	Width	Required	Data Element Description	Data Type	Acceptable Values	Definitions	Example
ParentEntityName	N/A	N/A	100	N	A unique number or alphanumeric code assigned to an organization by a school, school system, a state, or other agency or entity.	Alphanumeric/special xsd:token	One or more ASCII characters		IGroup1

3.9.3 Students

The Student upload file contains only student information; Accommodations and Explicit Eligibility information are added via separate uploads. However, student export combines student info plus any accommodations they have. Furthermore, there is no Explicit Accommodations export.

- **Change to user interface:** In order to manage the combinations of exports and output formats required, radio buttons will be added to the UI to allow the user to select the type of export: Students plus Accommodations, Students only, Accommodations only, and Explicit eligibility. Once an export type is selected, the user may select from one of the four search exports (all results to Excel, all results to CSV, current results to Excel, current results to CSV) (see Figure 8 and Figure 8).

Clicking on Export reveals new pane

Selecting required options reveals Submit button

Export

Export Current page Export all results

Select...

- ✓ Students Plus Accommodations
- Students
- Accommodations
- Explicit Eligibility

Male 2000-07-05

17

- Create two new export files with only student information and only accommodation information (with same columns as for import)
- Create new export with *ExplicitAccommodation* information.
- Create new export with *ExplicitEligibility* information.

3.9.4 Student Groups

- Change *Organization Name* in export to *ResponsibleDistrictIdentifier*.
- Change *Email Address* in export to *ElectronicMailAddress*.
- Change order of columns in export to match the import file
- Change Name of Institution in export file to *InstitutionIdentifier*.

3.9.5 Accommodations

In order to accommodate the flexible set of accommodations enabled by Task Order 10 (JIRA SB-1403), the following changes will need to be made:

- Consolidate all accessibility codes into one field (column) for both import and export formats.
 - This single-field-format will consist of a pipe-delimited list of (unique) accommodation codes for SingleSelect and Multiselect accommodation resource types.
 - For EditResource accommodation resource types, the format shall be **Code(value)**.
 - Example:

TDS_ASLE0|TDS_CCMagenta|TDS_ClosedCap1|TDS_PoD_Stim|editresource1(fluffy bunny)|other(blue light needed)

- Continue to accept upload of the multiple-column format used in the July 2015 release to maintain backward compatibility. (Note that the July 2015 import format has fixed column names and the format is not sensitive to the configuration file which is introduced with Task Order 10.)
- Update the ART file upload specifications (located at <http://www.smarterapp.org/specs/ART-Upload.html> and https://github.com/SmarterApp/smarterapp.github.io/blob/master/_original_documents/ART_File_Upload_Spec.docx)

4 Risks

Risk	Mitigation
Users could delete themselves out of the system	<ul style="list-style-type: none"> • Adequate confirmation mechanisms in place to prevent accidental deletion of roles and accounts by the user.

Smarter Balanced Test Delivery System High Level Requirements – Task Order 15

Risk	Mitigation
if a coordinator locks an account that also has roles outside their domain, the other roles would also be disabled (since the user can't authenticate). Likewise on the unlock – roles outside their domain would be enabled.	<ul style="list-style-type: none">• Adequate confirmation mechanisms in place to prevent accidental deletion of roles and accounts by the user.